

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
- Czynniki ludzkie

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)

```
root@zuw:~  
----- ettercap 0.6.b -----  
SOURCE: ANY <----- dryad (passive scanning) - ettercap  
DEST : ANY <-----  
----- 20 hosts in this LAN (212.14.59.242 : 255.255.255.192) -----  
54) 192.33.4.12 NL  
55) 192.36.148.17 NL  
56) 192.58.128.30 NL  
57) 192.112.36.4 NL  
58) 192.168.1.100 NL  
59) 192.203.230.10 NL  
60) 193.0.14.129  
61) 193.59.201.35  
62) 194.204.159.1  
63) 196.41.0.4  
64) 200.31.75.162  
65) 200.86.82.197  
66) 200.138.71.117  
67) 201.22.25.122  
68) 202.12.27.33  
69) 210.42.88.252  
70) 211.45.60.1  
71) 211.129.90.69  
72) 212.14.1.62  
73) 212.14.54.145  
74) 212.14.59.195  
75) 212.14.59.209  
76) 212.14.59.237  
77) 212.14.59.239  
78) 212.14.59.241  
79) 212.14.59.242  
80) 212.14.59.254  
81) 212.77.100.101 NL  
82) 212.77.100.133 NL  
83) 213.180.130.200 NL  
84) 213.241.71.158 NL  
85) 216.201.227.194 NL  
86) 217.172.33.106 NL  
-----  
Host Details :  
IP & MAC address : 212.14.59.242 00:0E:7F:24:4B:2E  
HOSTNAME : zuw.szczecin.uw.gov.pl  
FINGERPRINT : 16D0:05B4:40:WS:0:0:1:0:A:2C  
OPERATING SYSTEM : Linux 2.4.xx  
NETWORK ADAPTER : unknown  
DISTANCE IN HOP : 0  
OPEN PORTS (tcp) : 25 smtp  
: 80 http  
: 17721  
OPEN PORTS (udp) : NONE  
-----  
Your IP: 212.14.59.242 MAC: 00:0E:7F:24:4B:2E Iface: eth0 Link: SWITCH
```

network sniffing (ettercap)

```
root@zuw:~  
----- ettercap 0.6.b -----  
SOURCE: ANY <----- dryad (passive scanning) - ettercap  
DEST : ANY <-----  
----- 20 hosts in this LAN (212.14.59.242 : 255.255.255.192) -----  
54) 192.33.4.12 NL  
55) 192.36.148.17 NL  
56) 192.58.128.30 NL  
57) 192.112.36.4 NL  
58) 192.168.1.100 NL  
59) 192.203.230.10 NL  
60) 193.0.14.129  
61) 193.59.201.35  
62) 194.204.159.1  
63) 196.41.0.4  
64) 200.31.75.162  
65) 200.86.82.197  
66) 200.138.71.117  
67) 201.22.25.122  
68) 202.12.27.33  
69) 210.42.88.252  
70) 211.45.60.1  
71) 211.129.90.69  
72) 212.14.1.62  
73) 212.14.54.145  
74) 212.14.59.195  
75) 212.14.59.209  
76) 212.14.59.237  
77) 212.14.59.239  
78) 212.14.59.241  
79) 212.14.59.242  
80) 212.14.59.254  
81) 212.77.100.101 NL  
82) 212.77.100.133 NL  
83) 213.180.130.200 NL  
84) 213.241.71.158 NL  
85) 216.201.227.194 NL  
86) 217.172.33.106 NL  
-----  
Host Details :  
-----  
TCP SERVICES BANNER :  
  
25 220 zuw.szczecin.uw.gov.pl ESMTTP Sendmail 8.12.8/8.12.8; Tue, 14 Oc  
t 2008 23:26:04 +0200  
80 Apache/2.0.40 (Red Hat Linux)  
17721 SSH-1.99-OpenSSH_3.5p1  
-----  
Your IP: 212.14.59.242 MAC: 00:0E:7F:24:4B:2E Iface: eth0 Link: SWITCH
```

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

IANA — Cross-Pollination Scan - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

http://recursive.iana.org/

Często odwiedzane Pierwsze kroki Aktualności


Internet Assigned Numbers Authority

[Domains](#) [Numbers](#) [Protocols](#) [About IANA](#)

Cross-Pollination Check

The discovery of a [highly-effective cache poisoning attack](#) that can affect name servers providing recursive name service has made it important that such servers be patched to mitigate against the problem. Furthermore, the risk of cache poisoning for servers that share recursive and authoritative functions can cross-pollinate the authoritative function with incorrect data. This tool is designed to assess the authorities for a given domain and determine whether they provide vulnerable recursive service.

Provide a **domain name** to analyse

Safe.
The servers tested for ZACHODNIOPOMORSKIE.EU appear to not be vulnerable to cache poisoning.

Name server	IP Address	Results
SERVER.SZCZECIN.UW.GOV.PL	212.14.59.241	Appears to not respond to recursive lookups
ZUW.SZCZECIN.UW.GOV.PL	212.14.59.242	Appears to not respond to recursive lookups

Zakończono

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