

Ćwiczenie 3. Testy penetracyjne - rekonesans

Wykonał: Grzegorz Pol

Komputer: 237-16

Przedmiotem mojego zainteresowania była domena: www.mypegatus.pl

Rys. 1 (poniżej) Obrazy okien przeglądarki WWW zawierające dane uzyskane z serwera WHOIS:
https://hrd.pl/pcenter/partner_frame/whois.php

Domena	
Domena	mypegatus.pl
Id abonenta	hmns99306 (FIRMOWA)
Serwery nazw	dns.home.pl. [62.129.252.30] dns3.home.pl. [81.210.44.122] dns2.home.pl. [213.25.47.166]
Utworzona	2005.09.22 18:09:10
Ostatnia modyfikacja	2009.09.16 12:43:16
Opcja	brak
Registral	Home.pl sp.j. pl. Rodła 9 70-419 Szczecin Polska/Poland +48.914325555 +48.801445555 info@home.pl
Abonent	
Firma	Floors Tomasz Pol
Ulica	Listopadowa 1
Miasto	02-496 Warszawa
Lokalizacja	PL
Ostatnia modyfikacja	2010.03.02

Rys. 2 (poniżej) Obrazy okien przeglądarki WWW zawierające dane uzyskane z serwera WHOIS:
<http://whois.domaintools.com/>

Registrant Search: **"Mypegasus.pl"**

Email Search: info@home.pl is associated with about **228,912 domains**

Whois History: **5 records** have been archived **since 2009-07-08** .

Reverse IP: **72,338 other sites** hosted on this server.



[Log In](#) or [Create a FREE account](#) to start monitoring this domain name



DomainTools for Windows®

Now you can access domain ownership records anytime, anywhere... **right from your own desktop!** [Find out more >](#)

```
DOMAIN:                mypegasus.pl
registrant's handle:   hmns99306 (CORPORATE)
nameservers:          dns.home.pl. [62.129.252.30]
                     dns3.home.pl. [81.210.44.122]
                     dns2.home.pl. [213.25.47.166]

created:              2005.09.22 18:09:10
last modified:       2009.09.16 12:43:16
```

no option

```
REGISTRAR:
Home.pl sp.j.
pl. Rodla 9
70-419 Szczecin
Polska/Poland
+48.914325555
+48.801445555
info@home.pl
```

Rys. 3 (poniżej) Lista wszystkich autorytatywnych serwerów DNS badanej domeny

- 1. dns.home.pl. [62.129.252.30]**
- 2. dns3.home.pl. [81.210.44.122]**
- 3. dns2.home.pl. [213.25.47.166]**

Rys. 4 (poniżej) Obrazy okien programu *tracert* uzyskane w czasie badania osiągalności wszystkich autorytatywnych serwerów DNS badanej domeny

1. 62.129.252.30

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>tracert /?

Sposób użycia: tracert [-d] [-h maks_przes] [-j lista_hostów] [-w limit_czasu]
                [-R] [-S adres_źródłowy] [-4] [-6] nazwa_celu

Opcje:
-d                Nie rozpoznawaj adresów jako nazw hostów.
-h maks_przes    Maksymalna liczba przeskoków w poszukiwaniu celu.
-j lista_hostów  Swobodna trasa źródłowa według listy lista_hostów
                  (tylko IPv4).
-w limit_czasu   Limit czasu oczekiwania na odpowiedź w milisekundach.
-R              Śledź ścieżkę błędzenia (tylko IPv6).
-S adres_źródłowy Adres źródłowy do użycia (tylko IPv6).
-4              Wymuś używanie IPv4.
-6              Wymuś używanie IPv6.

C:\Documents and Settings\Administrator>tracert 62.129.252.30

Trasa śledzenia do dns.home.pl [62.129.252.30]
przewyższa maksymalną liczbę przeskoków 30

  1      9 ms      4 ms      3 ms    10.3.237.254
  2     45 ms     24 ms     16 ms    hp8212-gw-ita.wat.edu.pl [10.0.0.13]
  3     26 ms     19 ms     33 ms    elf.wat.edu.pl [10.0.0.2]
  4     25 ms     44 ms     42 ms    193.105.35.254
  5    148 ms    201 ms    111 ms    BemCORE-do-WAT.net.aster.pl [212.76.38.65]
  6      *        *         *        Upłynął limit czasu żądania.
  7      *        *         *        Upłynął limit czasu żądania.
  8      *        *         *        Upłynął limit czasu żądania.
  9     69 ms     47 ms     76 ms    dns.home.pl [62.129.252.30]

Śledzenie zakończone.

C:\Documents and Settings\Administrator>\
Nazwa '\' nie jest rozpoznawana jako polecenie wewnętrzne lub zewnętrzne,
program wykonywalny lub plik wsadowy.

C:\Documents and Settings\Administrator>\
Nazwa '\' nie jest rozpoznawana jako polecenie wewnętrzne lub zewnętrzne,
program wykonywalny lub plik wsadowy.

C:\Documents and Settings\Administrator>
```

2. 81.210.44.122

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Wersja 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 81.210.44.122

Trasa śledzenia do dns3.home.pl [81.210.44.122]
przewyższa maksymalną liczbę przeskoków 30

  1      9 ms    12 ms    3 ms    10.3.237.254
  2      7 ms    69 ms   43 ms   hp8212-gw-ita.wat.edu.pl [10.0.0.13]
  3     51 ms    57 ms   82 ms   elf.wat.edu.pl [10.0.0.2]
  4     68 ms    96 ms   21 ms   193.105.35.254
  5     16 ms    56 ms    *      BemCORE-do-WAT.net.aster.pl [212.76.38.65]
  6      *      *      *      Upłynął limit czasu żądania.
  7     15 ms    24 ms    3 ms   Netia.plix.pl [195.182.218.13]
  8     14 ms    15 ms   30 ms   WarsB010RT06-WarsH002RT22.inetia.pl [83.238.250.177]
  9     33 ms    31 ms   42 ms   WarsH002RT22-StarH001RT09.inetia.pl [83.238.251.33]
 10     28 ms    47 ms   61 ms   StarH001RT09-SzczC001RT01.inetia.pl [83.238.249.185]
 11     75 ms    70 ms   28 ms   83.238.253.198
 12     24 ms    38 ms   31 ms   213-17-221-58.ip.netia.com.pl [213.17.221.58]
 13     28 ms    40 ms   18 ms   dns3.home.pl [81.210.44.122]

Śledzenie zakończone.

C:\Documents and Settings\Administrator>
```

3. 213.25.47.166

```
C:\WINDOWS\system32\cmd.exe
Śledzenie zakończone.

C:\Documents and Settings\Administrator>tracert 213.25.47.166

Trasa śledzenia do dns2.home.pl [213.25.47.166]
przewyższa maksymalną liczbę przeskoków 30

  1      3 ms     2 ms     4 ms    10.3.237.254
  2     80 ms   113 ms   37 ms   hp8212-gw-ita.wat.edu.pl [10.0.0.13]
  3     23 ms   109 ms  150 ms   elf.wat.edu.pl [10.0.0.2]
  4    134 ms    36 ms    50 ms   193.105.35.254
  5      *    156 ms  193 ms   BemCORE-do-WAT.net.aster.pl [212.76.38.65]
  6      *      *      *      Upłynął limit czasu żądania.
  7    352 ms   141 ms  193 ms   z-atman.aster.net.pl [77.79.192.237]
  8     87 ms    80 ms    54 ms   z-atman.tpnet.pl [194.204.176.121]
  9     80 ms    55 ms    62 ms   szcz-ar1.tpnet.pl [195.117.0.142]
 10    132 ms   403 ms  753 ms   80.50.27.126
 11     66 ms   147 ms   93 ms   dns2.home.pl [213.25.47.166]

Śledzenie zakończone.

C:\Documents and Settings\Administrator>
```

Rys. 5 (poniżej) Obrazy okien programu *nslookup* uzyskane w czasie realizacji próby uzyskania zawartości pliku strefowego z dwóch wybranych, autorytatywnych serwerów DNS badanej domeny

```
C:\WINDOWS\system32\cmd.exe - nslookup
> server dns.home.pl
Default Server:  dns.home.pl
Address:  62.129.252.30

> set type=any.
unknown query type: any.
> set type=any
> mypegasus.pl
Server:  dns.home.pl
Address:  62.129.252.30

mypegasus.pl
  primary name server = dns.home.pl
  responsible mail addr = admin.home.pl
  serial = 1261949014
  refresh = 10800 (3 hours)
  retry = 3600 (1 hour)
  expire = 604800 (7 days)
  default TTL = 3600 (1 hour)
mypegasus.pl  internet address = 212.85.96.95
mypegasus.pl  nameserver = dns3.home.pl
mypegasus.pl  nameserver = dns2.home.pl
mypegasus.pl  nameserver = dns.home.pl
mypegasus.pl  MX preference = 10, mail exchanger = mypegasus.pl
dns.home.pl   internet address = 62.129.252.30
dns2.home.pl  internet address = 213.25.47.166
dns3.home.pl  internet address = 81.210.44.122
>
```

```
C:\WINDOWS\system32\cmd.exe - nslookup
> set type = any
Unrecognized command: set type = any
> set type=any
> mypegasus.pl
Server:  dns2.home.pl
Address:  213.25.47.166

mypegasus.pl  nameserver = dns.home.pl
mypegasus.pl  internet address = 212.85.96.95
mypegasus.pl  nameserver = dns2.home.pl
mypegasus.pl
  primary name server = dns.home.pl
  responsible mail addr = admin.home.pl
  serial = 1261949014
  refresh = 10800 (3 hours)
  retry = 3600 (1 hour)
  expire = 604800 (7 days)
  default TTL = 3600 (1 hour)
mypegasus.pl  MX preference = 10, mail exchanger = mypegasus.pl
mypegasus.pl  nameserver = dns3.home.pl
dns.home.pl   internet address = 62.129.252.30
dns3.home.pl  internet address = 81.210.44.122
dns2.home.pl  internet address = 213.25.47.166
>
```

Rys. 6 (poniżej) Obrazy okien programu *nslookup* uzyskane w czasie realizacji próby uzyskania zawartości rekordów MX, CNAME, TXT z dwóch wybranych, autorytatywnych serwerów DNS badanej domeny

```
C:\WINDOWS\system32\cmd.exe - nslookup
dns.home.pl      internet address = 62.129.252.30
dns3.home.pl     internet address = 81.210.44.122
dns2.home.pl     internet address = 213.25.47.166
> exit

C:\Documents and Settings\Administrator>nslook
Nazwa 'nslook' nie jest rozpoznawana jako polecenie wewnętrzne lub zewnętrzne,
program wykonywalny lub plik wsadowy.

C:\Documents and Settings\Administrator>nslookup
Default Server:  hyrlata.ita.wat.edu.pl
Address:  10.3.57.1

> server dns.home.pl
Default Server:  dns.home.pl
Address:  62.129.252.30

> set type=mx
> mypegasus.pl
Server:  dns.home.pl
Address:  62.129.252.30

mypegasus.pl    MX preference = 10, mail exchanger = mypegasus.pl
mypegasus.pl    internet address = 212.85.96.95
>
```

```
C:\WINDOWS\system32\cmd.exe - nslookup
Server:  dns.home.pl
Address:  62.129.252.30

mypegasus.pl    MX preference = 10, mail exchanger = mypegasus.pl
mypegasus.pl    internet address = 212.85.96.95
> exit

C:\Documents and Settings\Administrator>nslookup
Default Server:  hyrlata.ita.wat.edu.pl
Address:  10.3.57.1

> server dns2.home.pl
Default Server:  dns2.home.pl
Address:  213.25.47.166

> server type=any
*** Can't find address for server type=any: Server failed
> set type=mx
> mypegasus.pl
Server:  dns2.home.pl
Address:  213.25.47.166

mypegasus.pl    MX preference = 10, mail exchanger = mypegasus.pl
mypegasus.pl    internet address = 212.85.96.95
>
```

Rys. 7 (poniżej) Obrazy okien przeglądarki WWW uzyskane w czasie realizacji próby uzyskania zawartości rekordów MX, CNAME, TXT z dwóch wybranych autorytatywnych serwerów DNS badanej domeny

Wkleić obrazy okien

WŁASNE SPOSTRZEŻENIA I WNIOSKI:

Nie udało mi zrealizować wszystkich podpunktów wymaganych. Podpunkty, które wykonałem pokazują jak wiele informacji o stronach, administratorach jest jawnie dostępnych pobierając je całkowicie anonimowo.