hakin9

Zbieranie informacji do testów penetracyjnych

Błażej Kantak

Magazyn *hakin9*, Software-Wydawnictwo, ul. Piaskowa 3, 01-067 Warszawa, *pl@hakin9.org*

Praktyka

Zbieranie informacji do testów penetracyjnych

Błażej Kantak

stopień trudności

Podanie do publicznej wiadomości zbyt dużej ilości informacji może naruszyć zasad polityki bezpieczeństwa, a tym samym ułatwić atak na system informatyczny przedsiębiorstwa lub organizacji. Zobaczmy, gdzie i w jaki sposób łatwo znajdziemy cenne dane, które mogą posłużyć do kompromitacji systemu firmowych zabezpieczeń.

Pentesty. To ostatnio bardzo popularne hasło w prasie branżowej. Dla wielu osób, które swą wiedzę opierają na filmach typu *The Hackers,* gdzie włamanie do systemu informatycznego polega na latani u w rzeczywistości wirtualnej pomiędzy półprzeźroczystymi, świecącymi wieżami, pentesty to istna *czarna magia*. Okazuje się, że *diabeł nie taki straszny*... Wystarczy znajomość kilku narzędzi i metod pracy, aby, przy odrobinie szczęścia, doprowadzić do kompromitacji wybrany system zabezpieczeń.

W artykule nie mam zamiaru wykładać ani teorii hackingu, ani pisać o etyce, którą kieruje się i której przestrzega prawdziwy hacker. Artykuł ten nie będzie również prostym przewodnikiem po narzędziach, ani listą typu TODO. Zamierzam pokazać, jak wiedza, którą posiada lub może zdobyć większość obytych z komputerami i siecią użytkowników, odpowiednio skorelowana i zebrana może posłużyć do złamania systemu zabezpieczeń dużej części obecnych w Internecie firm i instytucji.

Postaram się pokazać, co można zrobić przy pomocy przeglądarki, krzesła, muzyki i oczywiście... własnej głowy, bez której wszystko inne, nawet to, co zawarte jest w tym tekście, pozostaje bezużyteczne. Celowo nie podam wszystkich szczegółów technicznych, aby Czytelnik mógł sam, na własną rękę poeksperymentować i poczuć satysfakcję z faktu, że coś może w końcu *się udać*.

Tekst ten skierowany jest przede wszystkim do użytkowników początkujących w dziedzinie bezpieczeństwa informatycznego, ale obytych z komputerami i Internetem. A zatem zaczynamy.

Jak sobie pościelesz...

Na początku napomknąłem o czynnikach warunkujących, w większości przypadków, końco-

Z artykułu dowiesz się...

- Jak wygląda pierwsza faza testów penetracyjnych,
- Jak należy się bronić przed pasywnym zbieraniem informacji.

Powinieneś wiedzieć...

- powinieneś umieć korzystać z przeglądarki internetowej,
- powinieneś znać model sieci TCP/IP,

Testy penetracyjne

Testy penetracyjne (audyt zabezpieczeń) to proces sprawdzania systemu zabezpieczeń infrastruktury informatycznej przez grupę wykwalifikowanych i upoważnionych osób, poprzez symulowanie różnych działań i akcji, które mogą zostać podjęte przez potencjalnego intruza. Celem testów jest zatem przeprowadzenie kontrolowanego ataku na systemy produkcyjne, wykrycie luk i ich eliminacja, a w końcowym rozrachunku podniesienie poziomu bezpieczeństwa informatycznego danego podmiotu (firmy bądź instytucji).

Ze względu na zasoby wiedzy, jaką może posiadać zespół pentestowy, testy dzieli się na tzw. black box testing, czyli zerowa wiedza o audytowanym obiekcie i white box testing – wgląd we wszystkie szczegóły techniczne (konfiguracje, dostęp do baz danych, kodu źródłowego itd.). Istnieje również podział ze względu na lokalizację audytorów, a więc testy zewnętrzne, przeprowadzane spoza badanego obiektu (np. sieci) i wewnętrzne – z punktu widzenia np.: Pracownika.

Każdy test penetracyjny dzieli się na fazy:

- Pasywne zbieranie informacji – proces wyszukiwania i zbierania danych dotyczących badanego obiektu w sposób pasywny, a więc nie dostarczając testowanemu celowi (np. firmie) żadnych przesłanek, że jest on inwigilowany;
- Skanowanie i mapowanie sieci – badanie tras ruchu, badanie reguł firewalla (ang. firewalking);
- Fingerprinting – identyfikacja rodzajów i wersji systemów informatycznych używanych w sieci;
- Wykrywanie luk i słabości konfiguracyjnych – analiza zebranych danych i określenie potencjalnych wektorów ataku;
- Włamanie – wykorzystanie słabości i przełamanie systemu zabezpieczeń;
- Eskalacja uprawnień – zdobywanie uprawnień w poszczególnych systemach informatycznych;
- Raportowanie – zebranie wszystkich danych do postaci raportu, przeanalizowanie ich wraz z kierownictwem oraz działem technicznym badanego celu (np. firmy) i wskazanie potencjalnych metod poprawienia stanu bezpieczeństwa infrastruktury IT.

Pentesty doczekały się, już jako metodologia, własnego standardu: OSSTMM (*The Open Source Security Testing Methodology Manual*) Instytutu ISECOM (*The Institute for Security and Open Methodologies*). Więcej informacji na ten temat można znaleźć pod adresem: *http://www.isecom.org/osstmm/*.

wy sukces. Podstawą wszystkich pentestów jest wygodne i dobrze dostosowane do indywidualnych potrzeb środowisko. Dla mnie jego integralną (wręcz niezbędną) częścią jest ulubiona przeglądarka (*Firefox*), dobra (czyt. relaksująca) muzyka, ołówek, notes (z dużą ilością kartek) oraz wygodne krzesło lub fotel, w którym audytor spędza mnóstwo czasu. Czas to ostatni z elementów tej całej układanki i jego odpowiednia ilość może przesądzić, bardziej niż inne elementy, o ostatecznym wyniku naszych działań. Dla wygody przyjmijmy, że nasz horyzont czasowy wynosi nieskończoność (więcej czasu nie powinniśmy potrzebować). To pozwoli na skupienie się na bardziej istotnych kwestiach.

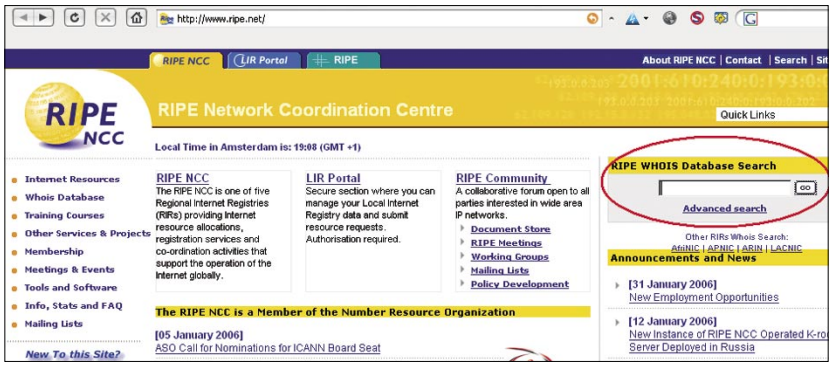
Po zapewnieniu sobie przyjaznego środowiska pracy, możemy zabrać się do konkretnej pracy. Nasze działania będą dotyczyły najwcześniejszej fazy testów penetracyjnych, a mianowicie pasywnego (względnie) zbierania informacji o potencjalnym celu (ang. *Passive Information Gathering* – zobacz w ramce Testy penetracyjne). Postawimy się w roli konsultanta ds. bezpieczeństwa, który otrzymał zlecenie zebrania jak największej ilości informacji o firmie (którą nazwiemy Nietykalni S.A.), nie zdradzając jednocześnie, że takowe informacje są zbierane.

Pomijamy tutaj zagadnienie, kto jest ewentualnym zleceniodawcą (może być to sama zainteresowana firma *Nietykalni S.A.*, bądź jej konkurencja). Jest to element kompletnie nie związany z samym zleceniem – my skupimy się wyłącznie na jego realizacji.

Low hanging fruits

Od czego zaczniemy? Niektórzy od razu odwiedziliby witrynę *www.nietykalnisa.com*, co kłóci się z naszym podstawowym postulatem – pozostawać w ukryciu. Jest w sieci wiele miejsc, w których można odnaleźć całe mnóstwo interesujących informacji o naszym obiekcie. Najczęściej są to serwisy, które powstały dawno temu i służyć miały ułatwieniu pracy użytkownikom korzystającym z sieci Internet. Jednakże, jak to często ma miejsce w całej historii ludzkości, okazało się, że *kij ma dwa końce*. Informacje takie, zebrane i właściwie zanalizowane, mogą pokazać dość wyraźny obraz tego, co się dzieje w firmie X, jaka jest jej struktura, z jakich dostawców korzysta, kto nią zarządza, kiedy pracuje itd. Można wymieniać bardzo długo. Oczywiście, nie w każdym przypadku uda się ustalić te wszystkie szczegóły, ale pomimo tego warto przynajmniej spróbować, ponieważ są to tzw. *low hanging fruits*, czyli coś, co można uzyskać bez większego wysiłku.

A więc dobrze. Zacznijmy od ustalenia, gdzie znajduje się firma *Nietykalni S.A.*, kiedy jest otwarta, jaki jest



Rysunek 1. *Witryna RIPE bazy WHOIS*

adres witryny oraz pozyskajmy ewentualnie numery telefonów kontaktowych. Zatem potrzebujemy książki telefonicznej. Ponieważ akurat nie musimy mieć pod ręką takowej (choć na najbliższej poczcie zapewne jest), w sieci dostępnych jest kilka witryn, które takie informacje podają: np. *Polskie Książki Telefoniczne* (*www.pkt.pl*), *Panorama Firm* (*www.pf.pl*) czy też *YellowPages* (*www.yellowpages.com*). Jeśli chcemy znaleźć lokalizację geograficzną wystarczy np. *www.pilot.pl, maps.google.com* lub *www.multimap.com*.

Warto zanotować wszystko to, co udało się ustalić. Przykładowo: numery telefonów kontaktowych mogą później posłużyć do ataków socjotechnicznych (jeśli będą wymagane) lub *wardialingu*, stosując podany przedrostek numeru. Adresy email pokazują, jaki jest stosowany format adresu (np.: *jas.fasola@nietykalnisa.com*).

Jeśli nasz obiekt (firma *Nietykalni S.A.*) jest notowany na giełdzie, można pokusić się o sprawdzenie, jakie informacje są udostępnione na witrynie Giełdy Papierów Wartościowych (*www.gpw.com.pl*) lub portalach finansowych (np.: *www.bankier.pl, www.money.pl* itp.).

Po zebraniu podstawowych informacji o naszej firmie sprawdźmy, co można odnaleźć w kilku innych miejscach. Zaczniemy od serwisu Whois.

Kto jest kto...

Whois jest bazą (patrz. Ramka *Serwis WHOIS*) o zarejestrowanych podmiotach internetowych i została stworzona z myślą o dostarczaniu informacji kontaktowych dla tych, którzy takich informacji potrzebują (np. przy konieczności skontaktowania się z administratorem danej sieci). Ponieważ my również należymy do tej grupy (pomimo tego, że nie chcemy się z nikim kontaktować z firmy *Nietykalni S.A.*), sprawdźmy, co w trawie piszczy.

W tym celu możemy skorzystać z popularnego narzędzia o nazwie whois, dostępnego w większości systemów linuxowych lub odpytać bazę WHOIS bezpośrednio z poziomu przeglądarki web (w naszym wypadku rejestr RIPE – *http://www.ripe.net/* – patrz Rysunek 1). Postawimy na drugą opcję, ponieważ jest ona bardziej uniwersalna i nie determinuje konieczności używania konkretnego systemu operacyjnego.

Listing 1. *Wyniki odpytania bazy WHOIS o nazwę firmy nietykalnisa.com*

```
% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
% The object shown below is NOT in the RIPE database.
% It has been obtained by querying a remote server:
% (whois.snd.pl) at port 43.
% To see the object stored in the RIPE database
% use the -R flag in your query
%
Domain object:
domain:          nietykalnisa.com
registrant's handle: msk9999 (CORPORATE)
nservers:        ns2.nietykalnisa.com.[10.14.86.33]
              ns1.nietykalnisa.com.[10.14.86.32]
created:         1999.12.02
last modified:  2005.12.13
registrar:       MLASK
ul. Ogórkowa 133
00-442 Słupsk
Polska/Poland
+48.22 5003333
help@snd.pl
option:          the domain name has not option
Subscribers Contact object:
company:         NIETYKALNI S.A.
street:          ALEJA PAWŁA I GAWŁA 150
city:            23-232 Oborkowo
location:        PL
handle:          msk9999
last modified: 2000.10.19
registrar:       MLASK
ul. Ogórkowa 133
00-442 Słupsk
Polska/Poland
+48.22 5003333
help@snd.pl
Whois database last updated: 2006.01.10
%%REFERRAL END
```

W zaznaczonym polu wpisać należy nazwę domeny (np.: *nietykalnisa.com*), nazwę konkretnego hosta (np.: *http://www.nietykalnisa.com/*) lub adres IP tego hosta.

My na początek zapytamy o domenę *nietykalnisa.com*.

Na Listingu 1 pokazano rekord dotyczący naszej firmy. Jak widać, Nietykalni S.A. korzystają z dwóch serwerów DNS o adresach 10.14.86.32 i 10.14.86.33, są zarejestrowani w MLASKu oraz mieszczą się w Oborkowie, co powinno pokrywać się z danymi, które uzyskaliśmy w pierwszym kroku. Jeśli nie, to najprawdopodobniej siedziba firmy uległa zmianie, połączyła się z inną lub jest to adres jednego z oddziałów, odpowiedzialnego za IT. Warto ten fakt zanotować.

Adresy serwerów DNS posłużą nam jako drugie zapytanie (o adres: 10.14.86.32 lub 10.14.86.33) do bazy WHOIS (Listing 2).

I cóż otrzymujemy? Po pierwsze, jaki blok adresów IP został przydzielony na potrzeby badanej firmy (10.14.86.0/24), kto jest osobą kontaktową (Jaś Fasola – kod JF6969-RIPE), adres, telefon, email oraz numer AS (AS12345). Ten ostatni wskazuje, czy Nietykalni S.A. mają zarejestrowany własny system autonomiczny, czy też korzystają z innego (w naszym przypadku podłączeni są do sieci WARIA.PL). Każda z tych informacji może zostać sprawdzona w bazie WHOIS i dostarczyć kolejnych, równie interesujących danych. I tu właśnie, drogi Czytelniku, zadanie dla Ciebie – sprawdź co można jeszcze wycisnąć z bazy RIPE (a jest tego trochę).

Ponieważ WHOIS nie jest jedynym miejscem, gdzie znajdziemy *nisko wiszące owoce*, nasz następny przystanek to znany wszystkim internautom serwis DNS, który może wprowadzić dużo zamieszania.

A Pan się zowie...

DNS to nic innego jak zbiór systemów serwujących odwzorowanie adresów IP na nazwy i odwrotnie. A więc tłumaczy zrozumiałe i łatwiejsze do zapamiętania przez człowieka nazwy na adresy numeryczne, wymagane w komunikacji w sieciach opartych na protokole IP. Co to dla nas oznacza? Umysł ludzki jest czasami przewidywalny i często kieruje się schematami lub przyzwyczajeniami. Przykładowo nazwa serwera WWW zaczynać się będzie od przedrostka www, firewalle często nazywane są *fw, DNSy – ns*, poczta – *mail* itp.

Administratorzy często posługują się zbiorem nazw wywodzących się z jednego korzenia, np. z mitologii, z astronomii (np. nazwy planet i ich księżyców) lub z przyjętego schematu (np. dhcp13-14 może oznaczać stację o adresie kończącym się na oktetach 13.14 i przypisywanym z serwera DHCP, bud01II122-01 – pierwszy komputer umieszczony w budynku nr 1 na II piętrze w pokoju 122.). To bardzo wygodne i ułatwia faktycznie administrowanie siecią, lecz pozostawia dużo niepotrzebnych informacji dla potencjalnego intruza. Czasami zdarza się nawet, że zewnętrzny serwer DNS tłumaczy nazwy komputerów znajdujących się w chronionej sieci!

Przy testach DNSa warto mieć pod ręką jakieś wygodne narzędzie. Pod systemem Linux standardowo dostępnych jest ich kilka (*dig, nslookup, host*), pod Microsoft Windows standardowo mamy do dyspozycji tylko jedno (*nslookup*). Pamiętajmy jednak, że mamy pozostawać w ukryciu. Dlatego lepiej jest użyć jakiejś witryny internetowej, która odpyta serwer DNS i zwróci nam wyniki bez konieczności wysyłania jakiegokolwiek pakietu w stronę obiektu naszych badań. Można w tym celu wykorzystać np. serwis *http://www.network-tools.com/*, który oferuje zaawansowane opcje odpytywania (Listing 2). Prześledźmy, co zwraca serwer DNS, gdy go odpowiednio zapytamy o domenę *nietykalnisa.com*.

Pierwsza rzecz, która rzuca się w oczy to fakt, iż serwerem administruje Wiktor Burak (widoczny w polu email: rekordu SOA) oraz, że podstawowym serwerem DNS jest serwer o hucznej nazwie Brodacz. Po przeanalizowaniu całego zapisu okazuje się, że serwer ten to nic innego jak NS1, zwrócony z bazy WHOIS oraz, że jego partner – NS2 – to *Lysy*, który jednocześnie jest serwerem pocztowym (rekord MX). To bardzo ważne informacje, ponieważ, jeśli serwery, które udostępniają tego typu usługi znajdują się na tej samej fizycznej maszynie, to wykryliśmy znaczące naruszenie zasad bezpieczeństwa. Skompromitowanie serwera pocztowego i zdobycie uprawnień jego superużytkownika jednocześnie oznacza przejęcie kontroli nad serwerem DNS, a to prowadzić może do bardzo poważnych konsekwencji!

Oczywiście, możliwe jest również, że pod tym samym adresem IP kryją się dwa różne fizyczne systemy. Może być to osiągnięte przez zastosowanie np.: *loadbalancingu* lub innego systemu przekierowującego zapytania do różnych usług.

Z jednego z rekordów TXT, który zawiera informacje tekstowe, możemy dowiedzieć się, że numer kontaktowy zmienił się (5005550). Może to oznaczać, że ktoś popełnił literówkę w czasie wpisywania danych do rekordu, co jest raczej mało prawdopodobne zważywszy, że cyfra *5* nie znajduje się w sąsiedztwie *0*, lub jest to numer do działu technicznego naszej firmy. I prawdopodobnie pracują tam: Jaś Fasola i Wiktor Burak. To nowe dane dla ewentualnego ataku socjotechnicznego.

Wracając do DNSa. Na stronie *http://www.ip-plus.net/tools/dns_check_set.en.html/* dostępne jest narzędzie, które w czasie odpytywania DNSa próbuje również ściągnąć cały plik strefy. Dziś bardzo niewiele serwerów jest podatnych na tego

Serwis WHOIS

Głównym zadaniem serwisu WHOIS jest dostarczenie informacji kontaktowych i rejestracyjnych danego podmiotu (firmy, instytucji, organizacji). Dzieli się on na dwie części – pierwsza odpowiada za informacje związane z danym zakresem adresów IP (tzw. *Network Service-based*), druga – z nazwami domenowymi (tzw. *Name Service-based*). Baza WHOIS zawiera m.in. adresy IP przydzielone do danego podmiotu, numer systemu autonomicznego (AS – wykorzystywanego do routingu BGP), dane osób odpowiedzialnych za utrzymanie wpisu oraz kilka innych.

Baza WHOIS została podzielona pomiędzy cztery Regionalne Rejestry (ang. *Regional Internet Regestries*):

- APNIC – Azja i Pacyfik (*Asia-Pacific Network Information Center*) – *http://www.apnic.net/*
- ARIN – Ameryka Płn. (*American Registry for Internet Numbers*) – *http://www.arin.net/*
- LACNIC – Ameryka Łacińska i Karaiby (*Latin American and Caribbean Internet Address Registry*) – *http://www.lacnic.net/*
- RIPE NCC – Europa (*Réseaux IP Européens Network Coordination Centre*) – *http://www.ripe.net/*

Listing 2. *Wyniki odpytania bazy WHOIS o adresacje IP firmy nietykalnisa.com*

```
% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag
% Information related to '10.14.86.0 - 10.14.86.255'
inetnum:        10.14.86.0 - 10.14.86.255
netname:        NIETYKALNIINTPL-NET1
descr:          Nietykalni
country:        PL
admin-c:        JF6969-RIPE
tech-c:         JF6969-RIPE
status:         ASSIGNED PA "status:" definitions
mnt-by:         WARIA-MNT
source:         RIPE # Filtered
person:         Jas Fasola
address:        Nietykalni S.A.
address:        Al. PAWŁA I GAWŁA 150
address:        23-232 Oborkowo
address:        POLAND
phone:          +48 55 5005555
fax-no:         +48 55 5005566
e-mail:         jas.fasola@nietykalnisa.com
nic-hdl:        JF6969-RIPE
source:         RIPE # Filtered
% Information related to '10.14.86.0/22AS12345'
route:          10.14.86.0/22
descr:          WARIA.PL
origin:         AS12345
mnt-by:         WARIA-MNT
source:         RIPE # Filtered
```

typu atak. Polega on na odczytaniu całej zawartości bazy podstawowego serwera DNS dla podanej domeny (w naszym przypadku *nietykalnisa.com*) jednym zapytaniem! Zwracane są wszystkie rekordy – nazwy stacji wraz z ich adresami IP. Takie dane są bardzo pomocne w określaniu struktury badanej sieci.

Można do problemu podejść też z drugiej strony. Jeśli mamy do czynienia z gorliwym administratorem, to każdy wpis w bazie podstawowej będzie odwzorowany w bazie odwróconej. Aby się dostać do tych informacji, wystarczy wysłać tzw. zapytanie odwrócone (ang. *reverse lookup*), tj. zapytać serwer DNS o nazwę dla podanego adresu IP. Czyli wysyłamy pytanie o znany adres IP (np. 10.14.86.32) i w odpowiedzi otrzymujemy przypisaną do niego nazwę (np.: *ns1.nietykalnisa.com, brodacz.nietykalnisa.com*). Przy odrobinie szczęścia możemy dostać prawie całą bazę DNS!

Ale żeby nie było łatwo załóżmy, że nasz admin jest strasznie zapracowany (bądź przesiaduje całymi dniami na IRC) i w efekcie bazy DNS są niekompletne. Pozostaje nam jeszcze najmniej elegancki sposób, jakim jest atak siłowy na DNS. Chodzi tu o proste zgadywanie. Możemy próbować zgadnąć, czy dana nazwa serwera nie występuje w bazie DNS (np.: *fw.nietykalnisa.com, ids.nietykalnisa.com, srv.nietykalnisa.com, srv1.nietykalnisa.com* itp.).

Analizując wcześniejsze wyniki można również spróbować zawęzić zakres poszukiwań i odpytać o nazwy, które są powiązane z już znanymi (np. postacie mitologiczne). W rozważanym przypadku mogą to być np.: *kudlacz.nietykalnisa.com, hipis.nietykalnisa.com, wasacz.nietykalnisa.com, loczek.nietykalnisa.com, czupiradlo.nietykalnisa.com* itp. Wszystko zależy od naszej inwencji i odrobiny wyobraźni.

Google is your friend...

No właśnie. Do tej pory korzystaliśmy z mniej popularnych źródeł informacji. Przejdźmy więc do tych bardziej oczywistych. Chyba każdy, kto czegokolwiek szukał w sieci, odwiedził witrynę *http://www.google.com/*. Jest to podstawowa przystań, jeśli chodzi o szukanie czegokolwiek w czymkolwiek. Nie bez przyczyny Google jest najlepszą wyszukiwarką internetową. Jej baza zawiera setki milionów odnośników, dokumentów, zdjęć i kontaktów. W numerze 3/2005 magazynu *hakin9* został opublikowany artykuł Michała Piotrowskiego pt.: *Niebezpieczne Google – wyszukiwanie poufnych informacji*, zatem nie będziemy tu ponownie omawiać technik znanych jako *google hacks*. Napomknę tylko o kilku drobnych szczegółach.

Wiadomo, że konstruując odpowiednio zapytania można uzyskać bardzo interesujące wyniki. Operatory typu: `site:`, `inurl:`, `intext:`, `intitle:` itd. ułatwiają wyszukiwanie danych i uściślają zakres przeszukiwania, a zatem wyniki są bliższe naszym oczekiwaniom. Tylko co zrobić w przypadku, gdy otrzymaliśmy ciekawy odnośnik? Gdy w niego klikniemy, nasz adres IP zostanie zapisany w logach badanego serwera WWW, a tego chcemy przecież uniknąć. Można skorzystać z darmowego serwera proxy (lista darmowych serwerów proxy dostępna jest np. pod www.proxy4free.com) lub pakietu Tor (*tor.eff.org*). Istnieje też bardziej eleganckie rozwiązanie.

Z pomocą przychodzi sam serwis Google, udostępniając nam swój cache (Rysunek 2). Większość stron

jest dostępna off-line, tj. nie musimy odpytywać docelowy serwer WWW, aby otrzymać stronę, która jest na nim hostowana. To co znajdziemy w cache'u, często jest wierną kopią strony pierwotnej. Ale jest tu mały haczyk. Jaki? Spójrzmy na Rysunek 3.

Zostało na nim przedstawione przykładowe zapytanie o witrynę magazynu *hakin9* i jej stronę dostępną z cache'a. Jednak, gdy prześledzimy logi Ethereala (Rysunek 4), uruchomionego w czasie ściągania tej strony okazuje się, że część zapytań została wysłana i odebrana z/od serwera WWW magazynu *hakin9* (adres 62.111.243.84)! A tego chcieliśmy uniknąć. Zatem co się stało?

Po krótkiej analizie odpowiedź jest banalna. Plik ze stylami CSS (pakiet 31) oraz kilka obrazków (pakiet 78, 80, 130 i następne) zawartych na stronie zostało ściągniętych z serwera źródłowego. Co zatem robić? W jaki sposób dostać się do cache'a bez zbędnego rozgłosu.

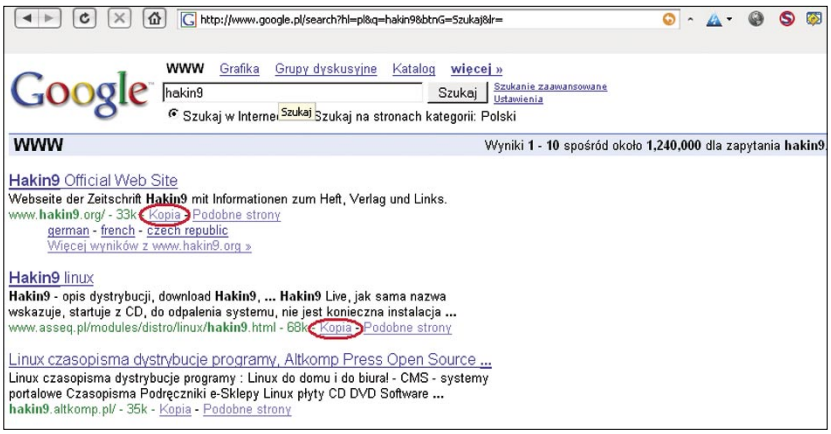
I znów Google nas zaskakuje. Gdy dokładnie przeczytamy nagłówek strony cache, to zauważymy napisany małym druczkiem komunikat o tym, że strona może zostać wyświetlona tylko w trybie tekstowym (Rysunek 5). Odnośnik do cache'a uległ małej zmianie. Na jego końcu pojawił się krótki parametr: &strip=1. To on odpowiada za naszą anonimowość. Zatem przy przeszukiwaniu cache'a wystarczy skopiować wynik wyszukiwania Google'a do schowka, wkleić w polu URL, dopisać magiczne &strip=1 i nacisnąć Enter. Proste i eleganckie.

Gdy mamy na myśli wyszukiwarki, zawsze na pierwsze miejsce automatycznie wysuwa się Google. Nie zapominajmy jednak, że istnieją jeszcze inne tego typu serwisy (*search.msn.com*, *www.yahoo.com*, *www.clusty.com*). Szczególnie polecam serwis Clusty, który, poza szybkością działania, ciekawie przedstawia wyniki końcowe, układając je w podkategorie (Rysunek 6).

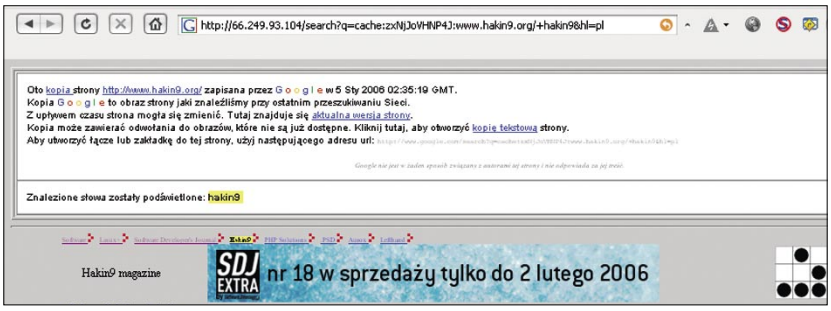
Pamiętajmy również o plikach *robots.txt* umieszczanych na serwe-

Listing 3. *Wyniki zapytania zwrócone przez serwer podstawowy DNS firmy nietykalnisa.com*

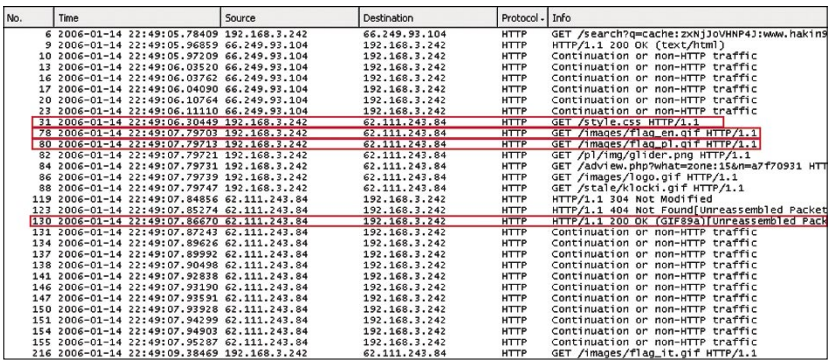
```
NsLookup Query the DNS for resource records
domain   query type  A - Address NS - Name server CNAME - Canonical name SOA
Start of authority MB - Mailbox domain MG -
Mail group member MR - Mail rename domain NULL - Raw data record WKS -
Well-known services PTR - Domain pointer HINFO - Host info MINFO - Mailing
list info MX - Mail exchange TXT - Text strings RP - Responsible person AFSDB
- AFS database X25 - X25 PSDN address ISDN - ISDN address RT -
Route through NSAP - NSAP address NSAP-PTR - NSAP-style pointer SIG -Security
signature KEY - Security key PX - X.400 mail mapping info AAAA - IPv6 address
LOC - Location NXT - Next domain SRV - Location of services NAPTR - Naming
authority pointer KX - Key exchange delegation UINFO -
User info UID - User ID GID - Group ID MAILB - Mailbox-related records ANY
                     - Any type
server   query class  IN - Internet CH - CHAOS HS - Hesiod ANY - Any class
port   timeout (ms)
 no recursion      advanced output
[10.14.86.32] returned an authoritative response in 156 ms:
Header
rcode: Success
id: 0 opcode: Standard query
is a response: True authoritative: True
recursion desired: True recursion avail: True
truncated: False
questions: 1 answers: 13
authority recs: 0 additional recs: 3
Questions
name class type
nietykalnisa.com ANY ANY
Answer records
name class type data time to live
nietykalnisa.com IN SOA server: brodacz.nietykalnisa.com
email: wiktor.burak@lysy.nietykalnisa.com
serial: 2005050508
refresh: 43200
retry: 3600
expire: 3600000
minimum ttl: 1209600
 8100s (2h 15m)
nietykalnisa.com IN NS lysy.nietykalnisa.com 8100s (2h 15m)
nietykalnisa.com IN NS brodacz.nietykalnisa.com 8100s (2h 15m)
nietykalnisa.com IN NS ns1.nietykalnisa.com 8100s (2h 15m)
nietykalnisa.com IN NS ns2.nietykalnisa.com 8100s (2h 15m)
nietykalnisa.com IN MX preference: 10
exchange: mail.nietykalnisa.com
 8100s (2h 15m)
nietykalnisa.com IN A 10.14.86.33 8100s (2h 15m)
nietykalnisa.com IN TXT Nietykalni S.A. 8100s (2h 15m)
nietykalnisa.com IN TXT Al. Pawla i Gawla 150 8100s (2h 15m)
nietykalnisa.com IN TXT FAX: +48 55 5005566 8100s (2h 15m)
nietykalnisa.com IN TXT TEL: +48 55 5005550 8100s (2h 15m)
nietykalnisa.com IN TXT 23-232 Oborkowo, POLAND 8100s (2h 15m)
nietykalnisa.com IN TXT RP: Admin <admin@nietykalnisa.com> 8100s (2h 15m)
Authority records
[none]
Additional records
name class type data time to live
lysy.nietykalnisa.com IN A 10.14.86.33 8100s (2h 15m)
brodacz.nietykalnisa.com IN A 10.14.86.32 8100s (2h 15m)
ns1.nietykalnisa.com IN A 10.14.86.32 8100s (2h 15m)
ns2.nietykalnisa.com IN A 10.14.86.33 8100s (2h 15m)
mail.nietykalnisa.com IN A 10.14.86.33 8100s (2h 15m)
-- end --
URL for this output
```



Rysunek 2. *Dostęp do cache'a serwisu Google*



Rysunek 3. *Strona cache serwisu Google*



No.	Time	Source	Destination	Protocol	Info
6	2006-01-14 22:49:05.78409	192.168.3.242	66.249.93.104	HTTP	GET /search?q=cache:zxNJoVHNP4J:www.hakin9
9	2006-01-14 22:49:05.96859	66.249.93.104	192.168.3.242	HTTP	HTTP/1.1 200 OK (text/html)
10	2006-01-14 22:49:05.97209	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
13	2006-01-14 22:49:06.03520	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
16	2006-01-14 22:49:06.03762	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
17	2006-01-14 22:49:06.04090	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
20	2006-01-14 22:49:06.10764	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
23	2006-01-14 22:49:06.11110	66.249.93.104	192.168.3.242	HTTP	Continuation or non-HTTP traffic
31	2006-01-14 22:49:06.30449	192.168.3.242	62.111.243.84	HTTP	GET /style.css HTTP/1.1
78	2006-01-14 22:49:07.79703	192.168.3.242	62.111.243.84	HTTP	GET /images/flag_en.gif HTTP/1.1
80	2006-01-14 22:49:07.79713	192.168.3.242	62.111.243.84	HTTP	GET /images/flag_pl.gif HTTP/1.1
82	2006-01-14 22:49:07.79721	192.168.3.242	62.111.243.84	HTTP	GET /pl/img/glider.png HTTP/1.1
84	2006-01-14 22:49:07.79731	192.168.3.242	62.111.243.84	HTTP	GET /adview.php?what=zone:15&n=a7f70931 HTT
86	2006-01-14 22:49:07.79739	192.168.3.242	62.111.243.84	HTTP	GET /images/logo.gif HTTP/1.1
88	2006-01-14 22:49:07.79747	192.168.3.242	62.111.243.84	HTTP	GET /stale/klocki.gif HTTP/1.1
119	2006-01-14 22:49:07.84856	62.111.243.84	192.168.3.242	HTTP	HTTP/1.1 304 Not Modified
123	2006-01-14 22:49:07.85274	62.111.243.84	192.168.3.242	HTTP	HTTP/1.1 404 Not Found[Unreassembled Packet
130	2006-01-14 22:49:07.86670	62.111.243.84	192.168.3.242	HTTP	HTTP/1.1 200 OK (GIF89a)[Unreassembled Pack
131	2006-01-14 22:49:07.87243	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
134	2006-01-14 22:49:07.89626	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
137	2006-01-14 22:49:07.89992	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
138	2006-01-14 22:49:07.90498	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
141	2006-01-14 22:49:07.92838	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
146	2006-01-14 22:49:07.93190	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
147	2006-01-14 22:49:07.93591	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
150	2006-01-14 22:49:07.93928	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
151	2006-01-14 22:49:07.94299	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
154	2006-01-14 22:49:07.94903	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
155	2006-01-14 22:49:07.95287	62.111.243.84	192.168.3.242	HTTP	Continuation or non-HTTP traffic
216	2006-01-14 22:49:09.38469	192.168.3.242	62.111.243.84	HTTP	GET /images/flag_it.gif HTTP/1.1

Rysunek 4. *Log z Ethereala pokazujący przyczynę odpytywania serwera źródłowego*

rach WWW w celu uniknięcia niepożądanego indeksowania niektórych stron. Każda wyszukiwarka posługuje się mechanizmem automatycznego przeczesywania i rejestrowania stron internetowych (tzw. *webcrawler*). *Webcrawler* analizuje odnaleziony kod HTML, wszystkie odnośniki w nim zawarte i stara się śledzić je dalej. Aby zapobiec indeksowaniu wybranych stron, w serwisie tworzony jest specjalny plik o nazwie *robots.txt*, w którym zawarte są instrukcje dla webcrawlera, które odnośniki ma pomijać. Jednakże sam plik *robots.txt* jest zapisywany – a to może dostarczyć kolejnych rodzynek w naszym pentestowych cieście. Takie małe, a jak cieszy.

Warto zajrzeć na grupy dyskusyjne. Czasami zdarza się, że administratorzy badanej przez nas sieci udzielają się w różnego rodzaju dyskusjach i forach. Odwiedzając *groups.google.com* szczególnie ciekawe mogą okazać się wypowiedzi personelu technicznego. Często zapytania o szczegóły techniczne jakiejś konfiguracji, bądź opisy problemów napotkanych w pracy pomogą nam określić, jakie systemy są wykorzystywane w firmie. Zdarza się, że częściowe konfiguracje urządzeń i serwisów mogą zostać ujawnione przez niefrasobliwych pracowników IT. W naszym przypadku należałoby szukać Jasia Fasoli i Wiktora Buraka, i sprawdzić czy nie wypowiadali się w jakiejś kontrowersyjnej sprawie (używając ich imion i nazwisk w kontekście nazwy *nietykalnisa.com*, bądź adresów email).

Częstą praktyką firm programistycznych i wdrożeniowych jest umieszczanie w swoim portfolio informacji o zakończonych i udanych projektach. I tu znaleźć możemy dane na temat systemów zainstalowanych wraz z szczegółami typu: rodzaj i wersja systemu operacyjnego, budowa sieci wewnętrznej, wersja bazy danych itd. Wszystkie te informacje, zanim zostaną umieszczone w Internecie, muszą być autoryzowane przez samego klienta. Zatem za jego zgodą tajemnica firmy zostaje ujawniona!

Co w sieci piszczy?

Co pozostaje nam poza wyszukiwarkami ? Całe mnóstwo możliwości.

Serwis Netcraft (*http://www.netcraft.com/*) dostarcza statystyki dotyczące witryn internetowych. Jednak informuje również o kilku innych, istotnych szczegółach. Przykładowo, pytając o stronę magazynu *hakin9* (Rysunek 7) otrzymujemy dane o lokalizacji, serwerze DNS, adresie IP, nazwie zwrotnej, systemie operacyjnym, na którym pracuje serwer web, a nawet informację o wersji tego serwera. Przy odpowiednim przepytaniu Netcrafta można odnaleźć niektóre nazwy DNS, których nie udało się uzyskać z serwera nazw (kolejne zadanie dla Czytelnika).

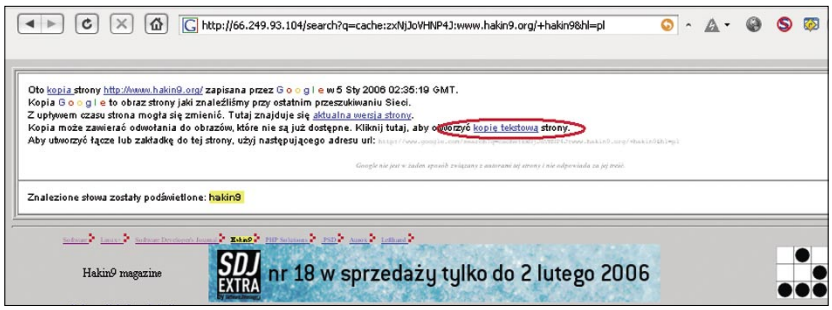
Walka ze spamem i bazy RBL (ang. *Realtime Blackhole List*) to również miecz obosieczny. Strona *openrbl.org* serwuje nam informacje o potencjalnych spammerach, ale udostępnia także interesującą nas funkcję: wyszukiwanie adresów email do zgłaszania spamu pochodzącego z danego adresu IP. Jeżeli w firmie została oddelegowana do tej funkcji specjalna osoba, to istnieje szansa, że ją poznamy. Zwiększy

się tym samym zakres naszych poszukiwań, ponieważ prawdopodobnie będzie to osoba z działu informatycznego.

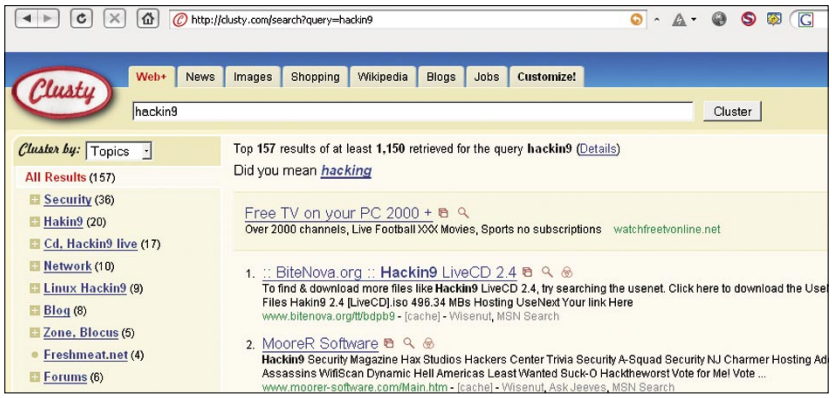
Istnieje również kilka witryn (np. *www.samspade.org, www.dnsstuff.com*), które dostarczają komplet narzędzi do szukania informacji (odpytywanie DNS proste i zwrotne, WHOIS, traceroute, ping itd). Przykładowo: DNSStuff pozwala nam przeprowadzać ataki typu email brute forcing. Jedno z narzędzi odpytuje serwer pocztowy, czy podany adres email zostanie zaakceptowany. Jeżeli odbiorca nie istnieje, zwracany jest błąd (Rysunek 8). W takim wypadku istnieją dwa wytłumaczenia: podany format adresu email jest niepoprawny, co raczej jest mało prawdopodobne, zważywszy na fakt, iż we wcześniejszych testach można było poznać właściwą formę zapisu lub dana osoba nie jest zatrudniona w danej firmie. Zatem znając format adresu email, korzystając ze słowników imion i nazwisk oraz z prostego skryptu można spróbować ustalić listę osób pracujących w firmie.

Należy jednak zwrócić uwagę na to, że takie uparte *pukanie do drzwi* może w końcu wzbudzić obudzić czyjąś czujność. Pomimo tego, że działamy pod przykrywką, nawet leniwy administrator czasami zagląda do logów. Jeżeli napotka mnóstwo nieudanych połączeń przychodzących z jednego adresu IP, zacznie się interesować, co się wydarzyło, a tego przecież nie chcemy. Dlatego zawsze używajmy każdego narzędzia z właściwym rozmysłem.

Warto w tym miejscu polecić oprogramowanie firmy *VisualWare*, które rysuje na mapie świata trasę z jednego punktu do drugiego. Na stronie *visualroute.visualware.com* jest dostępna wersja demo, lecz wymagana jest rejestracja. Można próbować się zarejestrować lub po prostu skorzystać z bazy *www.bugmenot.com*, na której dostępne są gotowe dane do uwierzytelnienia. Można również skorzystać ze strony *www.visualroute.pl*, która należy do GTS, jedynego dystrybutora oprogramowania *VisualWare* w Polsce.



Rysunek 5. *Cache Google z odnośnikiem do wersji tekstowej dokumentu*



Rysunek 6. *Wynik zwrócony przez serwis www.clusty.com*

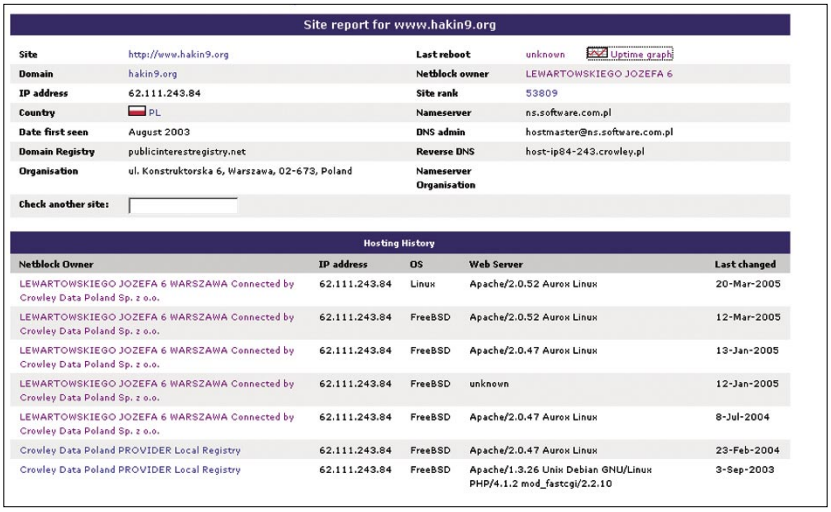
Masz wiadomość...

W numerze 5/2004 magazynu *hakin9* Tomasz Nidecki w artykule *Jak zdemaskować nadawcę listu* pisze o sposobach pozyskiwania informacji z nagłówków poczty elektronicznej. W nagłówkach tych zawarte są dane o trasie, jaką przebył list, jakie systemy pocztowe zostały wykorzystane, czy istnieje ochrona anywirusowa, antyspammowa, jakiego klienta poczty użył nadawca, jaka jest stosowana adresacja IP wewnątrz sieci firmowej itd. Wszystko to można dostać w prezencie w jednym emailu otrzymanym z badanego obiektu. Jak? Można skorzystać z darmowych kont pocztowych i wysłać zapytanie o nową ofertę handlową i spokojnie czekać na odpowiedź. Można również przeszukać fora internetowe w poszukiwaniu właśnie takich nagłówków.

Obrona

Przyszedł czas na wykopanie kilku fos i postawienie zasieków. Jak bronić się przed pasywnym zbieraniem informacji? Jakie działania podjąć w celu zminimalizowania wycieku danych? Oto kilka z zalecanych metod:

- nie zdradzać formatu emaila stosowanego wewnątrz organizacji – dotyczy to wszystkich adresów wykorzystywanych w celach technicznych – np. dla bazy WHOIS należy założyć osobną skrzynkę (*whois@nietykalnisa.com*);
- gdzie to tylko możliwe stosować jeden numer telefoniczny dla całej organizacji – trudniej będzie przez to zgadnąć zakres numerów przypisany przez operatora telekomunikacyjnego, co skutecznie utrudni atak typu wardialing;
- zablokować możliwość transferu pliku strefy z serwera DNS (większość dostępnego dziś oprogramowania serwerów DNS wyłącza tę funkcjonalność w swej domyślnej konfiguracji);
- odwzorowanie odwrotne DNS stosować tylko w uzasadnionych przypadkach;
- stosować nazwy DNS, które nie sugerują przeznaczenia danego serwera. Najlepiej jest przyjąć określony standard nazewniczy, w którym zawarte są dane jednoznacznie identyfikujące ho-



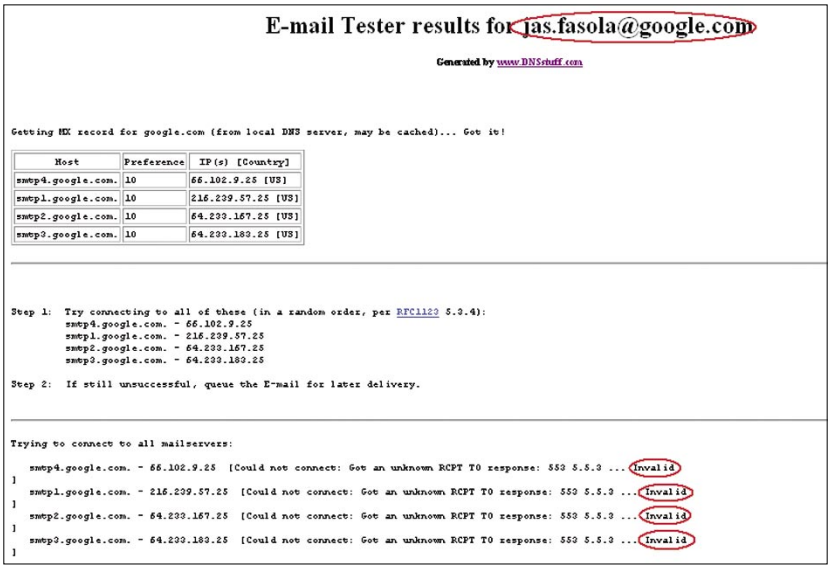
Site report for www.hakin9.org

Site	http://www.hakin9.org	Last reboot	unknown Uptime graph
Domain	hakin9.org	Netblock owner	LEWARTOWSKIEGO JOZEFA 6
IP address	62.111.243.84	Site rank	53809
Country	PL	Nameserver	ns.software.com.pl
Date first seen	August 2003	DNS admin	hostmaster@ns.software.com.pl
Domain Registry	publicinterestregistry.net	Reverse DNS	host-ip84-243.crowley.pl
Organisation	ul. Konstruktorska 6, Warszawa, 02-673, Poland	Nameserver Organisation	
Check another site:			

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
LEWARTOWSKIEGO JOZEFA 6 WARSZAWA Connected by Crowley Data Poland Sp. z o.o.	62.111.243.84	Linux	Apache/2.0.52 Aurox Linux	20-Mar-2005
LEWARTOWSKIEGO JOZEFA 6 WARSZAWA Connected by Crowley Data Poland Sp. z o.o.	62.111.243.84	FreeBSD	Apache/2.0.52 Aurox Linux	12-Mar-2005
LEWARTOWSKIEGO JOZEFA 6 WARSZAWA Connected by Crowley Data Poland Sp. z o.o.	62.111.243.84	FreeBSD	Apache/2.0.47 Aurox Linux	13-Jan-2005
LEWARTOWSKIEGO JOZEFA 6 WARSZAWA Connected by Crowley Data Poland Sp. z o.o.	62.111.243.84	FreeBSD	unknown	12-Jan-2005
LEWARTOWSKIEGO JOZEFA 6 WARSZAWA Connected by Crowley Data Poland Sp. z o.o.	62.111.243.84	FreeBSD	Apache/2.0.47 Aurox Linux	8-Jul-2004
Crowley Data Poland PROVIDER Local Registry	62.111.243.84	FreeBSD	Apache/2.0.47 Aurox Linux	23-Feb-2004
Crowley Data Poland PROVIDER Local Registry	62.111.243.84	FreeBSD	Apache/1.3.26 Unix Debian GNU/Linux PHP/4.1.2 mod_fastcgi/2.2.10	3-Sep-2003

Rysunek 7. *Wynik zapytania o domenę hakin9.org w serwisie Netcraft.com*



E-mail Tester results for jas.fasola@google.com

Generated by www.DNSstuff.com

Getting MX record for google.com (from local DNS server, may be cached)... Got it!

Host	Preference	IP(s) [Country]
smtp4.google.com.	10	66.102.9.25 [US]
smtp1.google.com.	10	216.239.57.25 [US]
smtp2.google.com.	10	64.233.167.25 [US]
smtp3.google.com.	10	64.233.183.25 [US]

Step 1: Try connecting to all of these (in a random order, per RFC1123 5.3.4):
smtp4.google.com. - 66.102.9.25
smtp1.google.com. - 216.239.57.25
smtp2.google.com. - 64.233.167.25
smtp3.google.com. - 64.233.183.25

Step 2: If still unsuccessful, queue the E-mail for later delivery.

Trying to connect to all mailservers:

smtp4.google.com. - 66.102.9.25 [Could not connect: Got an unknown RCPT TO response: 553 5.5.3 ... Invalid]
smtp1.google.com. - 216.239.57.25 [Could not connect: Got an unknown RCPT TO response: 553 5.5.3 ... Invalid]
smtp2.google.com. - 64.233.167.25 [Could not connect: Got an unknown RCPT TO response: 553 5.5.3 ... Invalid]
smtp3.google.com. - 64.233.183.25 [Could not connect: Got an unknown RCPT TO response: 553 5.5.3 ... Invalid]

Rysunek 8. *Błąd zwracany przez serwis DNSStuff.com przy podaniu niepoprawnego adresu email*

O autorze

Błażej Kantak od 15 lat interesuje się informatyką, a od ponad 8 jest z nią związany zawodowo. Obecnie pracuje, w randze *network troubleshootera*, dla dużej instytucji finansowej. Poza sieciami, które są jego główną specjalizacją, zajmuje się również zagadnieniami dotyczącymi bezpieczeństwa informatycznego, a w szczególności Wi-Fi, VPN, FW, VoIP i *psucie sprzętu* Cisco. Szuka również producenta koszulek z napisem: *My wife 0wnz me...* Ostatnim jego sukcesem z dziedziny Physical Security był udany DoS na windę.

sta z punktu widzenia np. inwentaryzacyjnego, ale nie będą zrozumiałe dla osoby spoza organizacji.

- ograniczyć rozgłaszanie banerów serwisów do minimum (np. SMTP, WWW itd) lub zmienić ich treść na taką, która będzie sugerować system inny niż w rzeczywistości. Czasami będzie to wymagało zmian w plikach konfiguracyjnych, a nawet w samym kodzie źródłowym, jeśli taki posiadamy (open source);
- wyłączyć zwracane komunikaty błędów na stronach WWW. Błędy takie mogą być wywoływane przez intruza przy pomocy nieprawidłowych danych wejściowych (np. wprowadzenie znaków w miejscu, gdzie wymagane są cyfry) i mogą zdradzać szczegóły samej aplikacji webowej (np. adresację IP sieci wewnętrznej, dostęp do i rodzaj bazy danych, hasła, etc.);
- jeśli jakaś strona zawierająca krytyczne lub poufne dane została zaindeksowana w wyszukiwarce, należy skontaktować się z obsługą techniczną w celu usunięcia tej strony z bazy i cache'a;
- nie autoryzować szczegółowych informacji o aktualnych i zakończonych wdrożeniach we własnej infrastrukturze informatycznej;
- nie stosować robots.txt – w zamian ustanowić uwierzytelnianie do krytycznych stron WWW wraz z szyfrowaniem SSL.

Podsumowanie

Proces zabezpieczania systemów informatycznych nie kończy się na szczelnym skonfigurowaniu firewalla, *spatchowaniu* serwera pocztowego, zaktualizowania bazy antywirusowej i zapisywaniu logów. Proces ten w zasadzie nigdy się nie kończy. W każdej sytuacji należy zastanowić się, czy podanie do publicznej wiadomości zbyt dużej ilości informacji (np. o wdrożeniu systemu PKI w firmie) nie naruszy zasad polityki bezpieczeństwa, a tym samym bezpieczeństwa wszystkich pracowników i zasobów firmy.

W artykule starałem się pokazać, jak z pozoru błahe i mało istotne dane mogą sprawić, że kompromitacja systemu będzie znacznie prostsza. Wiedza, której intruz nie powinien posiąść pozwala mu na uderzenie w nasz najczulszy punkt. Pamiętajmy, że zabezpieczając swą infrastrukturę informatyczną musimy sprawić, aby wszystkie jej elementy były równie wytrzymałe na atak. Intruzowi do odniesienia sukcesu wystarcza tylko jeden, najsłabszy element. A jest nim najczęściej człowiek. ●