PRZEGLĄD TELEINFORMATYCZNY
NR 3, 2017

Rekonesans pasywny w testach penetracyjnych

Zbigniew SUSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
zbigniew.suski@wat.edu.pl

STRESZCZENIE: W artykule opisano ogólne zasady prowadzenia testów penetracyjnych. Skupiono się przede wszystkim na fazie rekonesansu pasywnego. Opisano wybrane metody i narzędzia stosowane w trakcie takiego rekonesansu. Przestawiono wybrane wyniki badań, których celem było zweryfikowanie przydatności niektórych metod i narzędzi.

SŁOWA KLUCZOWE: bezpieczeństwo, testy penetracyjne, rekonesans

1. Wstęp

Testy penetracyjne to działania praktyczne, które polegają na próbach naruszenia zasobów sieci komputerowej określonej organizacji, w celu oceny bezpieczeństwa tej sieci. Poprzez symulację ataku, można stwierdzić, czy i które elementy sieci mogą stanowić potencjalną lukę, umożliwiającą uzyskanie nieuprawnionego dostępu lub wyrządzenie szkody aktywom organizacji.

Testy penetracyjne mogą być przeprowadzane niezależnie lub jako część procesu zarządzania ryzykiem w organizacji.

Należy zauważyć, że bezpieczeństwo sieci zależy nie tylko od czynników, które są powiązane ze środowiskiem IT. Wobec tego niezbędne jest wdrożenie odpowiednich wymagań w zakresie bezpieczeństwa ogólnego, analizy ryzyka, modelowania zagrożeń, przeglądu kodu i wielu innych elementów.

Testy penetracyjne są uważane za ostatnią i najbardziej agresywną formę oceny bezpieczeństwa. Powinny być realizowane przez tzw. zaufaną stronę trzecią, czyli niezależną od zamawiającej organizacji firmę zewnętrzną,

zatrudniającą wykwalifikowanych specjalistów. Mogą być prowadzone z lub bez wcześniejszej wiedzy o badanej sieci.

Wynikiem testów penetracyjnych jest zwykle raport podzielony na kilka sekcji, które dotyczą słabości występujących w obecnym stanie środowiska podlegającego badaniu, oraz potencjalnych środków zaradczych i innych zaleceń odnośnie działań naprawczych.

Tematyce testów penetracyjnych poświęcono w ostatnich 10 latach wiele pozycji książkowych. Wykaz najciekawszych i prawdopodobnie najbardziej popularnych zamieszczono w wykazie literatury [1] do [6]. Wszystkie wskazane pozycje zawierają ogólną charakterystykę testów penetracyjnych, charakterystykę poszczególnych faz testów oraz opis wybranych narzędzi zalecanych do użycia. Niektóre pozycje [9] do [15] poświęcone są głównie wybranym, najbardziej przydatnym narzędziom. Zawierają one również pewne ogólne uwagi dotyczące przebiegu testów penetracyjnych. Tematyka testów penetracyjnych pojawia się również na egzaminach umożliwiających uzyskanie certyfikatów z zakresu bezpieczeństwa systemów IT. Znajduje to odzwierciedlenie w materiałach pomocniczych dla uczestników stosownych kursów [8], [16].

Testy penetracyjne można przeprowadzać na trzy sposoby [1], [6], [8]:

- test czarnej skrzynki (*black-box test*),
- test białej skrzynki (*white-box test*),
- test szarej/kryształowej skrzynki (*gray-box/crystal-box test*).

W przypadku testu czarnej skrzynki, tester nie ma żadnej wiedzy o badanej sieci. Na przykład, jeśli są to zewnętrzne testy czarnej skrzynki, tester może otrzymać adres strony internetowej lub adres IP i próbować złamać zabezpieczenia tak, jakby to zrobił złośliwy intruz. Stosując takie podejście, tester oceniający infrastrukturę sieciową nie będzie wiedział o wewnętrznych rozwiązaniach technologicznych wdrożonych w organizacji. Dzięki zastosowaniu wielu tzw. technik hakerskich ze świata rzeczywistego, realizuje kolejne fazy testów, w których istniejące luki mogą zostać ujawnione i ewentualnie wykorzystane. Idealnym byłoby ustalenie wszystkich możliwych ataków, które mogłyby spowodować naruszenie bezpieczeństwa celu. Tego typu testy są zwykle bardziej kosztowne niż testy białej czy szarej skrzynki.

W przypadku testu białej skrzynki, tester ma pełną wiedzę na temat sieci wewnętrznej. Tester, przed rozpoczęciem testów może otrzymać diagramy sieciowe lub listę systemów operacyjnych i wykorzystywanych aplikacji. Oczywiście nie jest to metoda reprezentatywna dla ataków z zewnątrz. Jednak jest najbardziej dokładna, zwykle daje najlepsze efekty, ponieważ prezentuje najgorszy scenariusz, w którym intruz ma pełną wiedzę na temat atakowanej sieci. Tester powinien posiadać wiedzę odnośnie wszystkich technologii wykorzystywanych w badanym środowisku. Możliwe jest wówczas dokonanie

przeglądu i krytycznej oceny luk bezpieczeństwa, przy minimalizacji wysiłku i wysokiej dokładności. Takie podejście zwykle przynosi badanej organizacji więcej korzyści w stosunku do podejścia czarnej skrzynki.

W czasie testu szarej lub kryształowej skrzynki tester symuluje pracownika funkcjonującego wewnątrz sieci. Tester dysponuje kontem w sieci wewnętrznej i standardowym dostępem do sieci (jak uprawniony pracownik). Tego typu test pozwala ocenić zagrożenia wewnętrzne wynikające z działań pracowników firmy.

W celu uporządkowania i sformalizowania działań realizowanych w czasie testów penetracyjnych, opracowano szereg metodyk prowadzenia takich testów [6], [7]. Do najbardziej popularnych należy zaliczyć:

- Open Web Application Security Project (OWASP);
- Web Application Security Consortium Threat Classification (WASC-TC);
- Penetration Testing Execution Standard (PTES);
- Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- EC-Council Licensed Penetration Tester methodology (LPT);
- Penetration Testing Framework (PTF);
- NIST PUB 800-115 – Technical Guide to Information Security Testing and Assessment.

Istnieją dokumenty, które wymieniane są w grupie metodyk, ale są właściwie tylko katalogami najczęściej popełnianych błędów lub zagrożeń. Można do nich m.in. zaliczyć:

- OWASP TOP 10 Project;
- SANS 20 Critical Security Controls.

W zasadzie niemal wszystkie znane metodyki testów penetracyjnych zbudowane są na podobnym modelu. Model ten zakłada kolejno występujące po sobie fazy, w których wykorzystywane są różnego rodzaju narzędzia. Etapy te nie muszą występować ściśle po sobie. Dane dostarczane przez narzędzia w konkretnej fazie, są wykorzystywane zwykle jako wejście dla fazy kolejnej. Zaleca się aby jak najmniej zaburzać porządek, ale w uzasadnionych sytuacjach można to zrobić. Najbardziej ogólny podział uwzględnia dwie fazy: fazę rozpoznania i fazę przeprowadzenia ataków. Podział ten jednak nie jest jednoznaczny i czasami działania faz rozpoznania są zaliczane do faz ataków i vice versa.

2. Rekonesans

Rekonesans jest pierwszą fazą testu penetracyjnego. Jej celem jest nieagresywne zbieranie informacji o badanej organizacji. W języku angielskim używany jest czasami termin *footprinting*. Aczkolwiek czasami termin ten używany jest również w szerszym znaczeniu i określa wszelkie działania rozpoznawcze, również bardzo agresywne. Jak widać nazewnictwo nie jest ustabilizowane, co niejednokrotnie sprawia duże kłopoty, zwłaszcza początkującym pentesterom.

Zbieranie informacji można zrealizować na dwa sposoby: aktywny i pasywny. W czasie aktywnego zbierania informacji ma miejsce, wprowadzanie ruchu sieciowego do sieci organizacji podlegającej badaniu. Innymi słowy oznacza to aktywne bezpośrednie oddziaływanie na sieć badanej organizacji. W przypadku metody pasywnej, informacje o badanej organizacji są gromadzone poprzez wykorzystanie usług firm trzecich, takich jak np. różne wyszukiwarki, m.in. Google. Podczas pasywnego rozpoznania nie są wysłane dane do systemów docelowych. Orężem napastnika są zasoby Internetu.

Nie ma sensu porównywanie tych dwóch sposobów (grup metod) w celu określenia, który jest lepszy. One są po prostu inne. Każdy sposób ma swoje zalety i wady. Stosując podejście pasywne, można zebrać mniej informacji, ale działanie będzie niewidoczne dla zespołu odpowiedzialnego za bezpieczeństwo badanej sieci. W takim przypadku jest bardzo trudne, jeśli nie niemożliwe, aby firma mogła określić, czy i kiedy intruz lub tester prowadzi pasywne rozpoznanie. Działalność ta jest związana z niskim ryzykiem wykrycia oraz potencjalnie wysoką nagrodą dla napastnika.

Stosując metodę aktywną można uzyskać więcej informacji, ale niektóre urządzenia mogą odnotować realizowane działania. Podczas testów penetracyjnych, faza rozpoznania może być wykonana kilka razy. Tylko taki sposób działania daje szansę na „kompletność gromadzonych informacji", jeżeli w ogóle można tutaj używać terminu kompletność.

Ilość danych dostępnych w Internecie jest oszałamiająca i przesiewanie sieci, aby znaleźć użyteczne informacje może być zadaniem trudnym i pracochłonnym. Istnieją jednak narzędzia, które pomagają w zbieraniu i sortowaniu tego bogactwa wiedzy.

Wielu ludzi nie zdaje sobie sprawy z bogactwa danych, które można znaleźć i które mogą zostać wykorzystane przez napastników. Informacje, które będzie można znaleźć będą się różnić w zależności od testowanego celu, ale zazwyczaj obejmują takie elementy, jak zakresy adresów IP, nazwy domen, adresy e-mail, publiczne dane finansowe, informacje organizacyjne, stosowane technologie, tytuły pracy, numery telefonów, i wiele innych. Czasem można nawet znaleźć poufne dokumenty lub informacje, które są łatwo przekazywalne do publicznej wiadomości za pośrednictwem Internetu.

Testy penetracyjne będą najbardziej skuteczne, gdy będziemy posiadać dużo wiedzy o badanym środowisku. Czasami informacja ta zostanie dostarczona przez korporację, dla której przeprowadzany jest test. Innym razem trzeba będzie wykonać rekonesans, aby uzyskać nawet najbardziej błahe informacje. Pierwszym krokiem w każdej pracy są badania. Im lepiej przygotujemy się do realizacji postawionego zadania, tym bardziej prawdopodobne jest to, że odniesiemy sukces.

Rekonesans jest zapewne jednym z ważniejszych etapów testu penetracyjnego. Im więcej czasu spędzamy na zbieranie informacji na temat badanej organizacji, tym bardziej prawdopodobne jest to, że odniesiemy sukces w późniejszych fazach. Jak na ironię, rekonesans jest również jednym z najczęściej pomijanych, niewykorzystanych i nierozumianych kroków w metodologii testów penetracyjnych.

Być może przyczyną takiego stanu rzeczy jest to, że testerzy nie są wystarczająco zapoznawani z koncepcją testów penetracyjnych i nie zdają sobie sprawy z tego, że porządne zbieranie informacji może mieć istotne znaczenie dla realizacji późniejszych etapów testu. Możliwe jest również, że ten etap jest pomijany, ponieważ jest najmniej "techniczny". Często ludzie, którzy są nowicjuszami postrzegają tę fazę jako nudną i niemierzalną. Nic nie może być dalsze od prawdy.

Dostępnych jest bardzo niewiele dobrych, zautomatyzowane narzędzi, które mogą być wykorzystane do przeprowadzenia rekonesansu. Dobry zbieracz informacji musi być jednocześnie hakerem, socjotechnikiem i prywatnym detektywem. Oprócz braku narzędzi, brak jest również dobrze zdefiniowanych zasad realizacji, co odróżnia także tę fazę od wszystkich pozostałych. Na przykład, kiedy mówimy o skanowaniu, to daje się zaobserwować pewien porządek i przejrzysty ciąg kroków, które muszą być zrealizowane w celu prawidłowego skanowania portów. Taki porządek trudno jest zdefiniować dla fazy rekonesansu.

Do typowych źródeł informacji wykorzystywanych podczas rekonesansu należy zaliczyć:

- strony internetowe,
- dokumenty publiczne z sądach i innych urzędach, formularze podatkowe,
- serwisy wyszukiwawcze,
- archiwa,
- konferencje, publikacje naukowe, raporty z badań,
- grupy dyskusyjne i spotkania użytkowników, blogi,
- partnerzy biznesowi,
- metadane ze zdjęć, plików, dokumentów itp.,

- śmietniki,
- wszelkie inne zasoby publiczne.

Typowe rodzaje uzyskiwanych informacji obejmują:

- adresy i nazwy serwerów DNS,
- zakresy adresów IP,
- wykorzystywane systemy operacyjne,
- wykorzystywane IDS i IPS,
- stosowane technologie (hard i soft – w tym języki programowania),
- typy stosowanych urządzeń sieciowych,
- dane teleadresowe, nazwy kont, adresy e-mail,
- adresy stron internetowych (w tym łącza do stron wewnętrznych i zewnętrznych),
- lokalizacja serwerów usług,
- drzewo katalogowe serwera WWW,
- standardy szyfrowania,
- pola i zmienne formularzy (również ukryte),
- metody wysyłania formularzy,
- oferowane usługi i produkty.

Wszystkie te informacje są niezwykle przydatne podczas przeprowadzania dalszego rozpoznania (przeprowadzanego po fazie rekonesansu) i późniejszego ataku.

3. Założenia dotyczące przeprowadzonego eksperymentu

Śledząc literaturę dotyczącą testów penetracyjnych można zauważyć, że stosunkowo niewiele jest pozycji, które można byłoby uznać za nowe, zwłaszcza jeżeli chodzi o wczesne fazy takich testów. Mogłoby to spowodować powstanie opinii, że przedstawiane w tej literaturze zagadnienia są już nieaktualne a opisywane narzędzia nieskuteczne. Wobec tego w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki WAT podjęto projekt, którego celem była weryfikacja opisywanych metod i narzędzi zalecanych do wykorzystywania w trakcie rekonesansu pasywnego w ramach testów penetracyjnych. Stosowne eksperymenty były przeprowadzane przez studentów specjalności „Cyberobrona" na kierunku „Kryptologia i cyberbezpieczeństwo". Dodatkowym uzyskanym efektem dydaktycznym było zapoznanie się studentów z praktyką w omawianym zakresie. Ograniczenie projektu do rekonesansu pasywnego wynikało z analizy możliwości realizacyjnych oraz ograniczeń prawnych.

Projekt polegał na próbach przeprowadzenia rekonesansu pasywnego w stosunku do wybranych domen dostępnych w Internecie. Wyboru domen dokonywali studenci. Jedyne ograniczenie dotyczące ich wyboru polegało na niedopuszczeniu do sytuacji, w której dwie lub więcej osób zajmowałoby się tą samą domeną. Badaniu poddano 23 domeny.

Przed przystąpieniem do działań rozpoznawczych, studenci uczestniczyli w cyklu wykładów poświęconych eksploracji sieci, rozumianej w tym przypadku jako uzyskiwanie informacji o zasobach sieci w czasie faz rozpoznawczych w teście penetracyjnym[1]. Zakres tematyczny wykładów nie był ograniczony jedynie do fazy rekonesansu.

4. Uzyskane wyniki

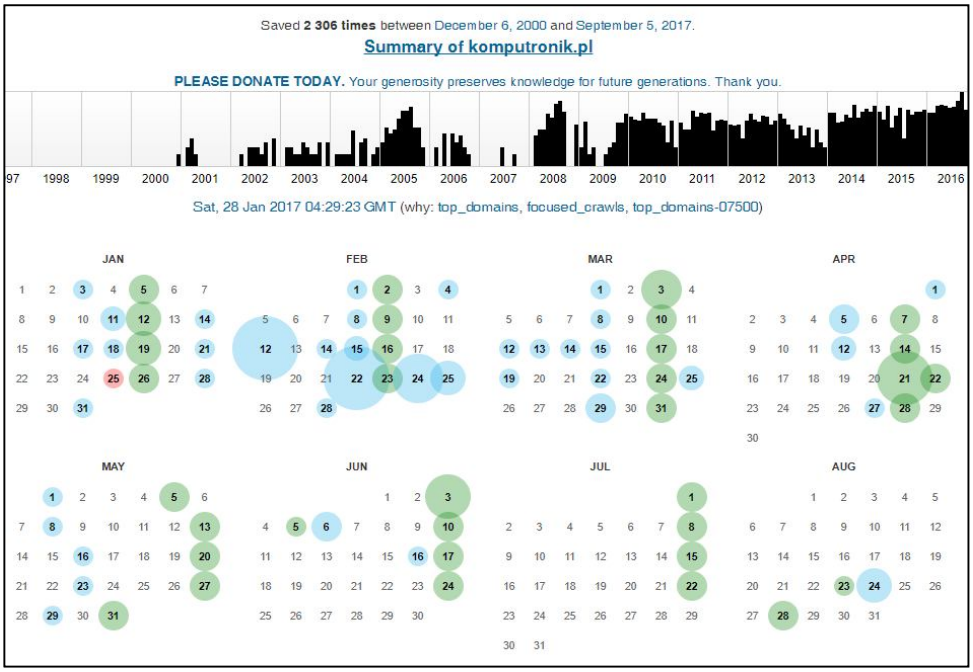
W niniejszym rozdziale przedstawione zostały wybrane, ciekawsze wyniki przeprowadzonych testów. Prezentacja wszystkich uzyskanych wyników nie jest możliwa ze względu na ich objętość.

4.1. Strona internetowa organizacji

Strona internetowa firmy jest dokumentem, od którego należy rozpocząć poszukiwanie i analizę informacji. Uzyskanie dostępu do takich stron i ich przeglądanie w trybie online oczywiście jest możliwe i na upartego można byłoby przyjąć, że nie łamie zasad rekonesansu pasywnego. Jednak bardziej skuteczna może okazać się analiza w trybie offline. Przede wszystkim pozwala ona na poświęcenie większej ilości czasu na poszukiwanie informacji. Darmowych i komercyjnych programów, które umożliwiają pobieranie całych drzew katalogowych stron z serwerów www, nie brakuje w Internecie. Jako przykład można podać programy *GNU Wget, Teleport Pro, HTTrack*.

Jednak zalecane podejście polega na pobraniu takich stron z dostępnych w Internecie zasobów archiwalnych. Z jednej strony wyklucza to bezpośredni dostęp do zasobów testowanej organizacji, co jest przecież jedną z naczelnych zasad rekonesansu pasywnego, z drugiej umożliwia przeprowadzenie analizy w trybie offline. Jak już powiedziano, pozwala to poświęcić więcej czasu analizie, bez zwiększania ryzyka wykrycia. W ten sposób, w procesie pobierania, można również czasami zbierać tzw. strony osierocone (ang. *orphan pages*). Są to strony, do których były zdefiniowane łącza, ale teraz już tych łączy nie ma. Takie strony powinny zostać usunięte z serwera, a czasami nie są. Mogą one zawierać informacje użyteczne dla pentestera.

1 Zastrzeżenie to wynika ze słownikowej niejednoznaczności terminu „eksploracja”.



Rys. 1. Fragment wykazu archiwalnych stron komputronik.pl w serwisie web.archive.org

Rys. 2. Fragment archiwalnej strony komputronik.pl (z dnia 14.07.2011) pozyskanej z serwisu web.archive.org

Na rysunku 1 przedstawiono fragment obrazu strony z serwisu web.archiwe.org prezentującej zasoby archiwalne tego serwisu dotyczące

witryny komputronik.pl. Można zauważyć, że zarchiwizowane zostały strony od roku 2000 (konkretnie od 6.12.2000). Na rysunku 2 przedstawiono fragment jednej ze stron archiwalnych komputronik.pl pozyskanej z serwisu web.archive.org.

Analizując wszystkie zarchiwizowane dokumenty można prześledzić nie zmiany wyglądu strony internetowej na przestrzeni lat, co jest jednak z punktu widzenia pentestera mało interesujące. Przede wszystkim często można uzyskać informacje, które nie są już dostępne w Google lub aktualnej wersji strony oraz dokonać szczegółowej analizy kodu. Biorąc pod uwagę liczbę zarchiwizowanych stron można sobie wyobrazić jak wielkiego nakładu pracy potrzeba aby dokonać gruntownej analizy, gdyż tylko w taki sposób można osiągnąć zadawalające efekty.

Strony internetowe zmieniają się z kilku powodów. Pentester najbardziej jest zainteresowany aktualizacjami, które służyły poprawieniu błędów takich jak ujawnienie wrażliwych informacji dotyczących serwera i sieci lub informacji osobistych. Prawdopodobnie już zostały usunięte. Z drugiej strony, informacje historyczne mogą już być nieaktualne.

Należy pamiętać, że niektóre zarchiwizowane strony mogą zawierać łącza do docelowego serwera WWW. Często jest to łącze dla uzyskania obrazów. Ponieważ zajmujemy się rekonesansem pasywnym, chcemy ukryć nasze zainteresowanie poprzez ograniczenie dostępu przeglądarki internetowej do tych obrazów. Wyłączenie realizacji automatycznych odwołań jest parametrem konfiguracyjnym przeglądarki.

Rys. 3. Dane kontaktowe osób na stronie organizacji

Przeglądając pobrane strony, należy zwrócić uwagę na 2 elementy: komentarze w kodzie źródłowym i informacje kontaktowe. Uzyskane informacje

kontaktowe (przykład na rysunku 3) mogą być użyte do dalszego zbierania informacji o wskazanych osobach np. na portalach społecznościowych. Są wówczas duże szanse odkrycia informacji bardzo osobistych, w tym kolejnych adresów funkcjonariuszy korporacyjnych, numerów telefonów domowych, informacji o członkach rodziny, zainteresowaniach.

Poprzez uzyskane adresy można trafić do osobistych stron internetowych pracowników, takich jak blogi, strony rodzinne lub pokrewne. Niektóre informacje mogą być pomocne intruzowi. Dotyczy to m.in. informacji o posiadanych certyfikatach inżynierów sieciowych potwierdzających znajomość systemów lub aplikacji oraz prawdopodobne ich wykorzystywanie w organizacji, w której pracują. Należy pamiętać to, że nie wszystkie zdobyte informacje są istotne. W poszukiwaniu informacji warto zachować równowagę między tym, co jest naprawdę pomocne, a tym co jest po prostu dostępne. Wszystkie zdobyte w ten sposób informacje mogą być następnie wykorzystane podczas ewentualnych ataków socjotechnicznych.

Analiza adresów mailowych pracowników może spowodować wykrycie w organizacji dodatkowych poddomen, którymi warto się zainteresować.

```
var MooTools={version:"1.2.5",build:"008d8f0f2fcc2044e54fdd3635341aaab274e757"};var
* @version             $Id: caption.js 5263 2006-10-02 01:25:24Z webImagery $
* @copyright    Copyright (C) 2005 - 2010 Open Source Matters. All rights reserved.
* @license             GNU/GPL, see LICENSE.php
* Joomla! is free software. This version may have been modified pursuant
* to the GNU General Public License, and as distributed it includes or
* is derivative of works licensed under the GNU General Public License or
* other free or open source software licenses.
* See COPYRIGHT.php for copyright notices and details.
*/

/**
* JCaption javascript behavior
*
* Used for displaying image captions
*
* @package      Joomla
* @since        1.5
* @version      1.0
*/
```

Rys. 4. Komentarz informujący o wykorzystaniu pakietu *Joomla* 1.5

Komentarze w kodzie źródłowym mogą ujawnić platformę, na której strona została osadzona. Może to być przydatne przy dalszej infiltracji serwera WWW. Komentarze mogą ujawnić również narzędzie wykorzystane do tworzenia strony (co pozwala łatwiej znaleźć stosowne eksploity). Komentarze mogą ujawnić również producenta strony. Może to ułatwić określenie platformy i stosowanej technologii

Rysunek 4 prezentuje komentarz z jednej ze stron badanej podczas opisywanego eksperymentu. Wynika z niego, że do tworzenia strony wykorzystano pakiet *Joomla* 1.5. Strona była archiwizowana 22.07.2017 roku.

Jak widać, nie zawsze wykorzystywane są najnowsze pakiety narzędziowe. W 2017 roku dostępny był już pakiet *Joomla* 3.7. Dla starszych wersji *Joomla* można znaleźć opublikowane exploity[2]. Bardzo często w kodzie stron można znaleźć informację o wykorzystywanych wtyczkach (ang. *plugin*). Biorąc pod uwagę, że dla nich również opisane mogą być stwierdzone podatności i nawet exploity, zaliczyć to można do cennych informacji, które jest w stanie pozyskać intruz.

Wreszcie, ważne jest, aby szukać i sprawdzić oferty pracy w badanej firmie. Oferty pracy często ujawniają bardzo szczegółowe informacje na temat technik wykorzystywanych przez organizację. Wielokrotnie będzie można znaleźć szczegóły odnośnie wykorzystywanego sprzętu i oprogramowania. Należy pamiętać, aby szukać swojego celu również w ogólnodostępnych bankach miejsc pracy. Załóżmy na przykład, że znajdziemy ofertę pracy dla administratora sieci z doświadczeniem w zakresie Cisco ASA. Z tego postu, można wyciągnąć wniosek, że firma albo korzysta lub ma zamiar wykorzystywać Cisco ASA firewall. Można również wywnioskować, że firma nie ma, lub prawdopodobnie utraci kogoś z wiedzą, jak właściwie korzystać i konfigurować Cisco ASA firewall. W obu przypadkach intruz zdobędzie cenną wiedzę na temat technologii w badanej organizacji.

4.2. Lista poddomen

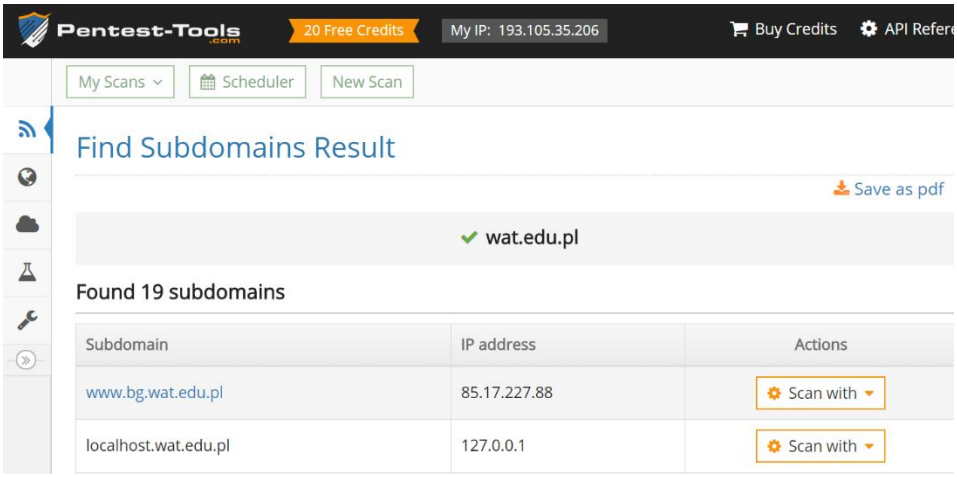
Często na podstawie nazwy organizacji łatwo jest odszukać nazwę jej domeny. Może ona jednak mieć strukturę zagnieżdżoną i może być z nią związanych kilka poddomen. Jeżeli lista poddomen nie okaże się pusta, to należy rozszerzyć poszukiwania i wykonać kolejną iterację rekonesansu. Tym razem w stosunku do wykrytych poddomen. Informację o strukturze domeny można uzyskać m.in. za pomocą witryn narzędziowych pentest-tools.com, narzędzia *knock.py*, *sublistr3r*, czy programu *robtex,* nazywanego przez niektórych scyzorykiem szwajcarskim. Trzeba jednak zwrócić uwagę, że wymienione narzędzia czasami zwracają jako nazwy poddomen, nazwy pojedynczych hostów. Wobec tego należy poddać uzyskane wyniki stosownej weryfikacji.

Na rysunku 5 przedstawiono fragment raportu prezentującego wyniki poszukiwania poddomen, zrealizowanego w ramach opisywanego eksperymentu. W liście poddomen znajdują się zarówno nazwy poddomen jak i nazwy pojedynczych hostów z badanej domeny.

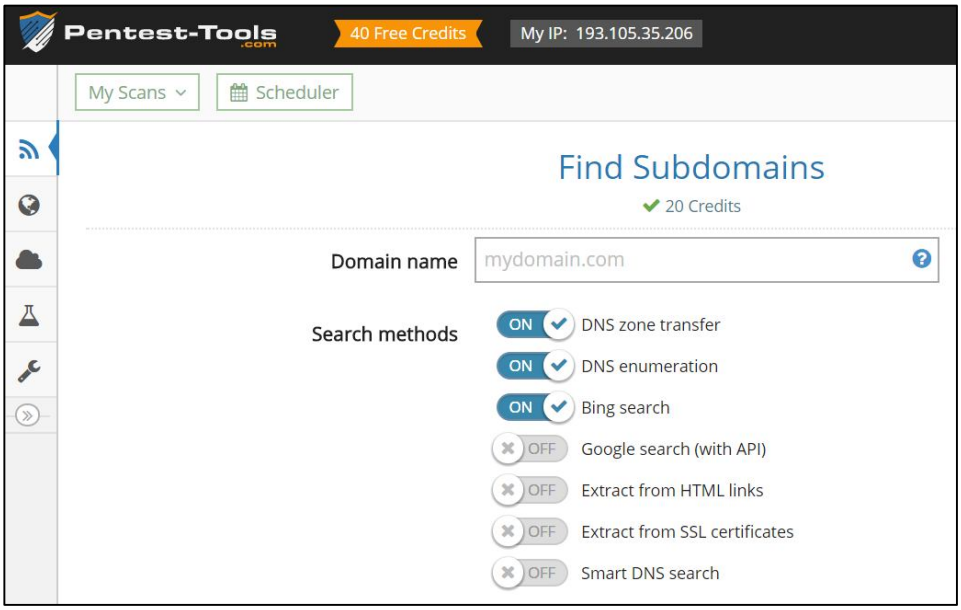
Większość dostępnych narzędzi nie umożliwia wyboru metody testowania. Należy zdawać sobie sprawę, że niektóre metody stosowane do

[2] Przykładowo: CVE-2010-5048, CVSS 4,3.

wykrywania poddomen przekraczają granice rekonesansu pasywnego. Niektóre mogą nie być akceptowane przez właściciela domeny i wówczas należy uzyskać jego zgodę na takie działanie.



Rys. 5. Fragment raportu prezentującego listę znalezionych poddomen



Rys. 6. Formularz umożliwiający wybór metody stosowanej podczas wyszukiwania poddomen

Rysunek 6 prezentuje formularz witryny pentest-tools.com, umożliwiający poszukiwanie poddomen i wybór metod, które powinny być stosowane. Można zauważyć, że niektóre z nich faktycznie przekraczają granice rekonesansu pasywnego

4.3. Usługa WHOIS

Bardzo prostym, ale skutecznym narzędziem do zbierania informacji o testowanej domenie jest usługa WHOIS. Usługa ta pozwala na dostęp do informacji takich jak adresy IP lub nazwy serwerów DNS oraz informacji kontaktowych, zazwyczaj zawierających adresy i numery telefonów.

Kiedy osoba lub podmiot prawny rejestruje nazwę domeny, podawanych jest wiele informacji. W zależności od ustawień zasad prywatności rejestracji można pozyskać te informacje i użyć ich do zweryfikowania przestrzeni IP, znaleźć informacje o innych miejscach należących do tej samej osoby lub korporacji, a nawet numery telefonów i adresy kluczowych pracowników. Ten rodzaj rekonesansu jest uważany z pasywny, ponieważ nie ma bezpośredniego kontaktu z zasobami właściciela domeny. Należy zlokalizować rejestratora, u którego domena została zarejestrowana w celu uzyskania przydatnych informacji. Ale nie zawsze jest to potrzebne.

Pierwotnie usługa WHOIS opracowana została jako narzędzie, za pomocą którego administratorzy systemów mogli w prosty sposób znajdować informacje umożliwiające skontaktowanie się z innymi administratorami, odpowiedzialnymi za serwery działające pod określonym adresem IP lub w określonej domenie. Teraz z tej usługi mogą korzystać wszyscy.

Aby skorzystać z usługi należy połączyć się z jednym z serwerów, które świadczą tą usługę. Najczęściej realizuje się to za pomocą przeglądarki. Można jednak użyć specjalnych programów. Np. polecenie *whois* jest wbudowane w system Linux.

W uzyskiwanych raportach znajduje się między innymi lista autorytatywnych serwerów DNS. Jeśli prezentowane są tylko nazwy serwerów, to trzeba będzie odwzorować te nazwy na adresy IP (np. poleceniem *host*).

Fragment jednego z raportów uzyskanego podczas eksperymentu przedstawiono na rysunku 7. Oprócz danych adresowych samej organizacji, widnieją w nim również nazwy serwerów DNS oraz dane osobowe administratora łącznie z numerem telefonu.

W celu ograniczenia nadużyć, coraz częściej bazy serwerów WHOIS są chronione przed systematycznym ich odpytywaniem. Ilość zwróconych danych lub ilość zapytań może być limitowana dla jednego adresu IP w przeciągu określonego czasu. Rejestrator domen najwyższego poziomu zwykle udziela

informacji tylko z własnej bazy WHOIS. Na przykład, ARINwhois, poszukuje tylko w swojej bazie i nie będzie szukał w bazie APNICwhois. Mogą funkcjonować jeszcze inne ograniczenia (np. *captcha*).

Zdarza się, że uzyskany raport nie dostarcza wielu szczegółów. Czasami można uzyskać dostęp do dodatkowych informacji, odpytując serwer WHOIS wymieniony w uzyskanym raporcie, jeżeli taki jest w nim wymieniony.

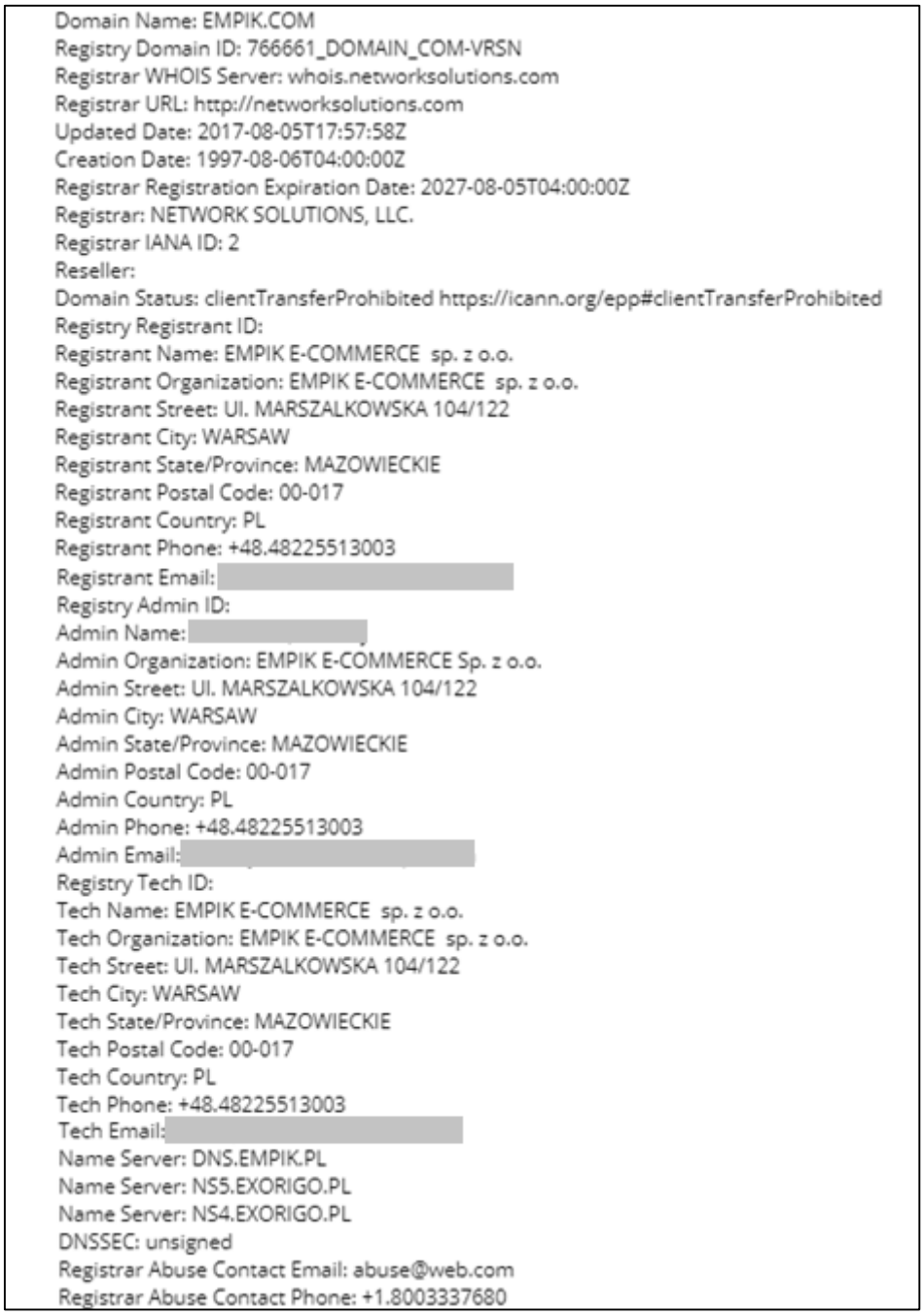
4.4. Media społecznościowe

Gwałtowny rozwój mediów społecznościowych takich jak Facebook, LinkedIn, GoldenLine, MySpace czy Twitter dostarcza nowych sposobów pozyskiwania danych. Dobrym pomysłem jest korzystanie z tych witryn podczas przeprowadzania rozpoznania. Szczególnie cenne są informacje dotyczące pracowników. Niektóre dane dotyczące pracowników można uzyskać metodami, które już zostały opisane w niniejszym opracowaniu. Wykorzystując media społecznościowe można taką wiedzę pogłębić.

Na rysunku 8 przedstawiono fragment danych administratora jednej z witryn badanych podczas eksperymentu. Dość dużym prawdopodobieństwem można założyć, że jego ścieżka zawodowa i certyfikaty, którymi się legitymuje, są związane z technologiami wykorzystywanymi w organizacji, w której aktualnie jest zatrudniony. Jeszcze więcej informacji dotyczących tej osoby znaleziono w zasobach serwisu GoldenLine.

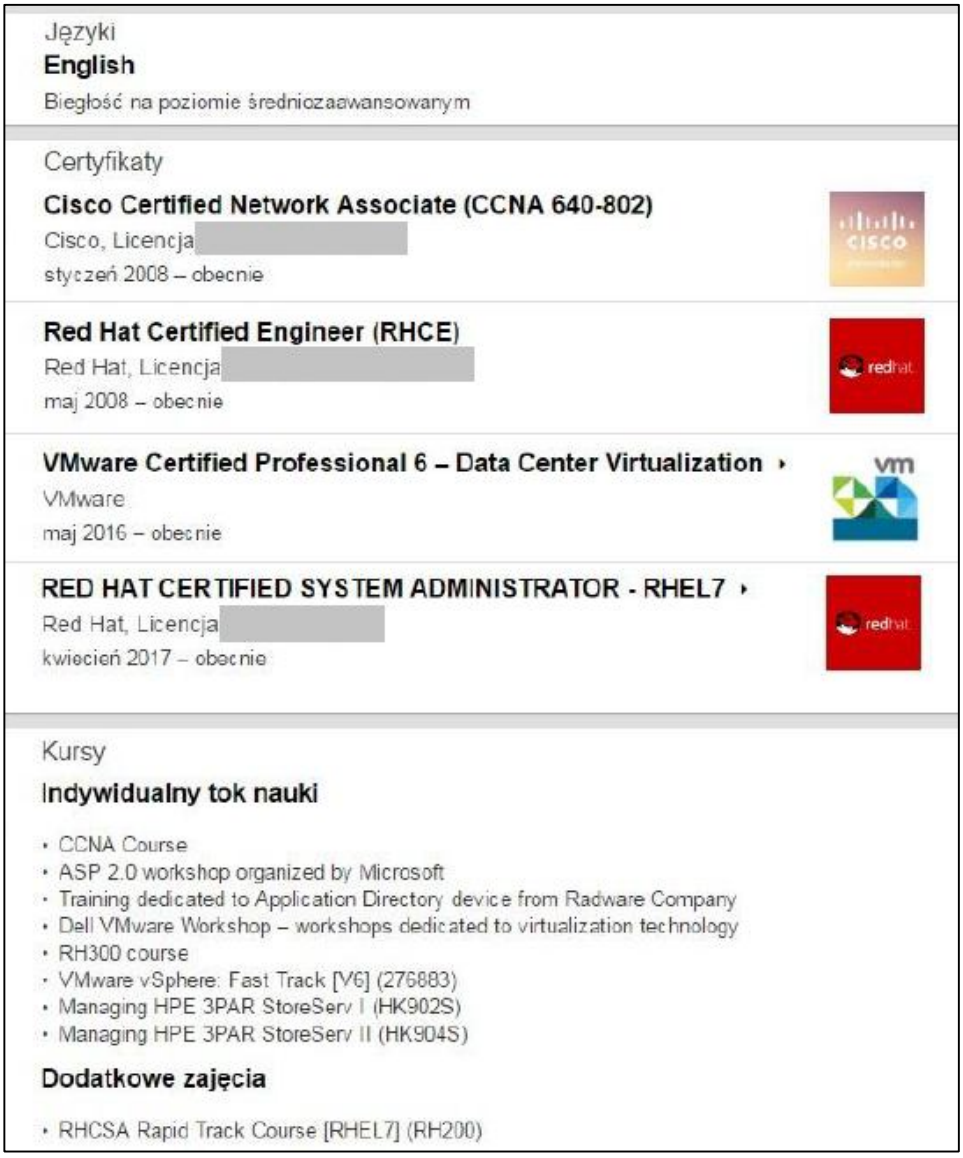
Dane początkowe umożliwiające poszukiwanie w serwisach społecznościowych szczegółowych informacji o kluczowych osobach w organizacji, można uzyskać z wielu źródeł. Zwykle są to tylko imiona i nazwiska takich osób. Ale jest to znakomity punkt zaczepienia dla dalszych poszukiwań. Godnymi uwagi są serwisy takie jak www.gpw.pl (rysunek 9) czy baza EDGAR w Stanach Zjednoczonych (rysunek 10).

W USA, notowane na giełdzie przedsiębiorstwa mają obowiązek składania pewnych dokumentów do Komisji Bezpieczeństwa i Giełd (SEC). Można uzyskać dostęp do tych informacji za pośrednictwem wspomnianej bazy danych EDGAR (http://www.sec.gov/edgar.shtml). Wyszukiwania może ujawnić informacje finansowe, dane osobowe istotnych pracowników i komunikaty prasowe. Niektóre firmy publikują dane odnośnie wykorzystywanych przez siebie technologii. Intruzowi może oszczędzić to czasu, potrzebnego na ustalenie danych osobowych ważnych pracowników, systemu operacyjnego i wykorzystywanego oprogramowania. Podobnie jest w innych krajach.

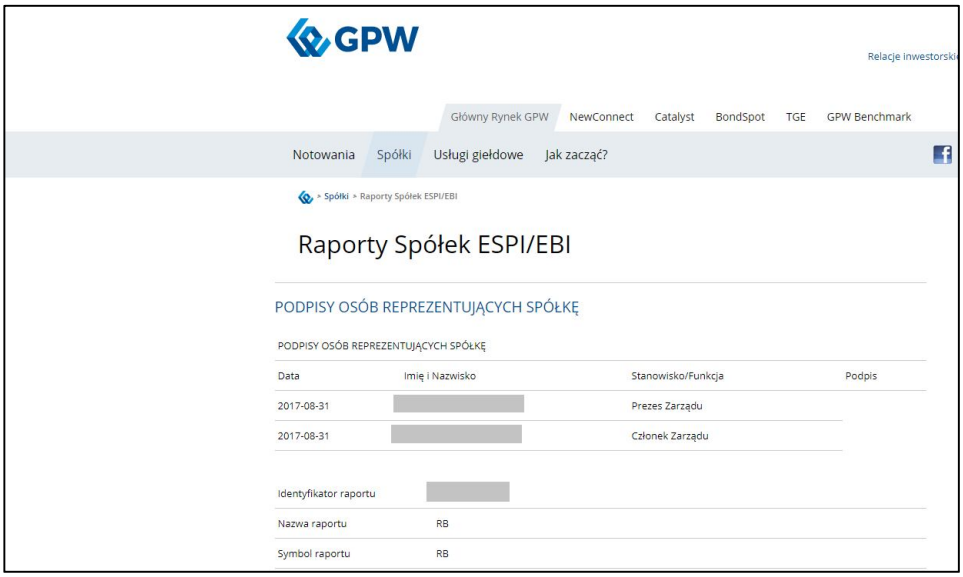


```
Domain Name: EMPIK.COM
Registry Domain ID: 766661_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-08-05T17:57:58Z
Creation Date: 1997-08-06T04:00:00Z
Registrar Registration Expiration Date: 2027-08-05T04:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: EMPIK E-COMMERCE  sp. z o.o.
Registrant Organization: EMPIK E-COMMERCE  sp. z o.o.
Registrant Street: Ul. MARSZALKOWSKA 104/122
Registrant City: WARSAW
Registrant State/Province: MAZOWIECKIE
Registrant Postal Code: 00-017
Registrant Country: PL
Registrant Phone: +48.48225513003
Registrant Email:
Registry Admin ID:
Admin Name:
Admin Organization: EMPIK E-COMMERCE Sp. z o.o.
Admin Street: Ul. MARSZALKOWSKA 104/122
Admin City: WARSAW
Admin State/Province: MAZOWIECKIE
Admin Postal Code: 00-017
Admin Country: PL
Admin Phone: +48.48225513003
Admin Email:
Registry Tech ID:
Tech Name: EMPIK E-COMMERCE  sp. z o.o.
Tech Organization: EMPIK E-COMMERCE  sp. z o.o.
Tech Street: Ul. MARSZALKOWSKA 104/122
Tech City: WARSAW
Tech State/Province: MAZOWIECKIE
Tech Postal Code: 00-017
Tech Country: PL
Tech Phone: +48.48225513003
Tech Email:
Name Server: DNS.EMPIK.PL
Name Server: NS5.EXORIGO.PL
Name Server: NS4.EXORIGO.PL
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
```

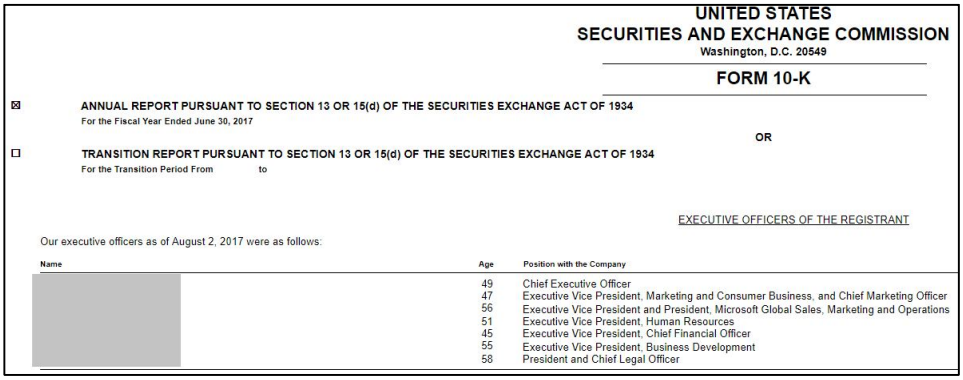
Rys. 7. Fragment raportu WHOIS



Rys. 8. Fragment danych administratora jednej z witryn badanych podczas eksperymentu (serwis LinkedIn)



Rys. 9. Fragment raportu giełdowego zawierający dane osobowe



Rys. 10. Fragment raportu z bazy EDGAR zawierający dane osobowe

4.5. Grupy dyskusyjne

Jedną z metod, której używa się do szukania pomocy jest zamieszczenie pytania na określony temat w grupie dyskusyjnej Usenet. Ludzie korzystają z tych forów dyskusyjnych, aby zgłaszać pytania i otrzymywać pomoc m.in. w kwestiach technicznych. Niestety (lub na szczęście, w zależności od punktu widzenia), pracownicy często zgłaszają bardzo szczegółowe pytania, zawierające w treści informacje wrażliwe lub wręcz poufne.

Jako przykład, rozważmy początkującego administratora sieci, który ma problemy z uzyskaniem prawidłowej konfiguracji wykorzystywanej zapory sieciowej. Nie jest niczym niezwykłym umieszczanie na forach zawartości całych plików konfiguracyjnych. Co gorsza, wiele osób w swoich postach używa firmowych adresów e-mail. Informacja taka jest wirtualną kopalnią złota dla intruza (lub testera).

Nawet jeśli administrator jest wystarczająco inteligentny, by nie zamieszczać plików konfiguracyjnych, to należy się liczyć z pewnym wyciekiem informacji. Ujawnione mogą zostać dane dotyczące wersji oprogramowania, modeli wykorzystywanego sprzętu, bieżące informacje konfiguracyjne i tym podobne. Wszystkie takie informacje mogą być wykorzystane przez intruza.

Fora publiczne są doskonałym narzędziem, aby dzielić się informacjami i otrzymywać pomoc techniczną. Jednak podczas korzystania z tych zasobów, należy uważać, aby używać nieco bardziej anonimowego adresu e-mail, zamiast adresu firmowego.

Listy różnego rodzaju grup można uzyskać m.in. pod adresami http://freenews.maxbaud.net/ oraz https://groups.google.com. Podczas opisywanego eksperymentu, tylko w jednym przypadku odnaleziono forum dotyczące badanej organizacji. Było ono jednak wykorzystywane głównie do wyrażania opinii dotyczących tej firmy. Ponieważ zdecydowanie dominowały opinie negatywne lub wręcz obraźliwe, w treści niniejszego artykułu nie został zamieszczony obraz tej listy.

4.6. Bazy danych spamu

W The Information Systems Security Assessment Framework (ISSAF) można znaleźć zapis, że cel należy zbadać w celu ustalenia, czy został on wymieniony w bazie danych spamu. Jeżeli obiekt jest wymieniony w tej bazie danych (a nie powinien), może to oznaczać, że serwer poczty elektronicznej został w przeszłości skompromitowany. Być może właściciel w dalszym ciągu ma z nim kłopoty. Dostęp do wspomnianej bazy można uzyskać poprzez adres www.dnsbl.info (rysunek 11). Żadna z badanych organizacji nie figurowała na „czarnej liście”

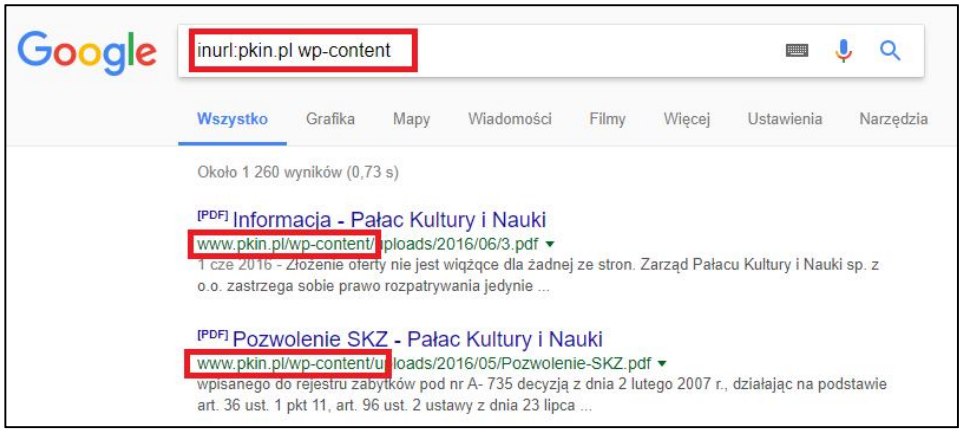
Rys. 11. Fragment strony prezentującej zawartość bazy spamu

4.7. Zaawansowane mechanizmy wyszukiwania Google

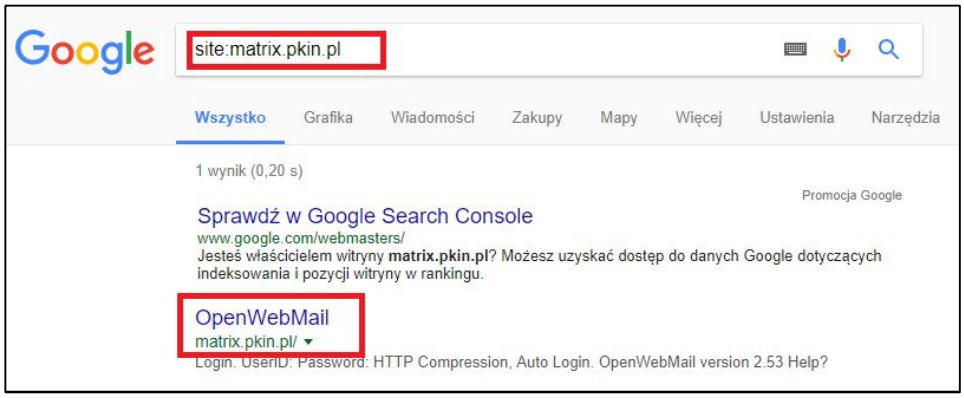
Zapytanie kierowane do Google może zawierać jedną lub kilka specjalnych dyrektyw, umożliwiających nakładanie dodatkowych warunków dotyczących poszukiwanych informacji. Wspomniane dyrektywy (operatory) pozwalają na budowanie bardzo ciekawych i przydatnych zapytań. Umożliwia to pozyskanie dodatkowych informacji o stronach przechowywanych w bazie danych wyszukiwarki.

Istnieje wiele książek na temat hackingu z wykorzystaniem Google. Zawarto w nich wiele szczegółowych opisów i „sztuczek" związanych z wykorzystaniem Google. Jedną z takich pozycji jest książka, której głównym autorem jest Johnny Lon [17]. GHDB (*Google hacking database*) jest źródłem ekspoitów (zapytań) zwiększających zasięg wyszukiwarki Google.

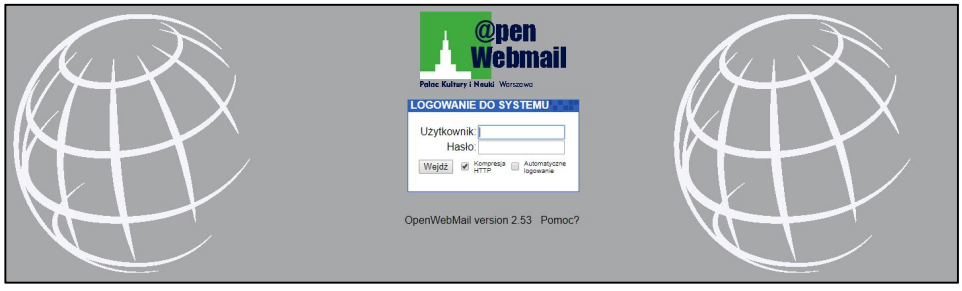
W trakcie eksperymentu testowano skuteczność tego mechanizmu. W przypadku domen, które podlegały badaniu rezultaty były mierne. W przypadku jednej z organizacji uzyskano informację, że wykorzystywana jest w niej platforma WordPress (rysunek 12). Zapytanie dotyczyło standardowego foldera o nazwie *wp-content*, wykorzystywanego w ramach platformy WordPress. Można zauważyć, że sformułowanie takiego zapytania może wymagać dość znacznej wiedzy odnośnie budowy i funkcjonowania pakietów programowych, których śladów poszukujemy. Zapytanie, którego wyniki przedstawiono na rysunku 13 pozwala stwierdzić, że pod adresem matrix.pkin.pl funkcjonuje system pocztowy OpenWebMail. Potwierdza to również odwołanie do tego adresu (rysunek 14). Adres matrix.pkin.pl został uzyskany podczas wcześniejszych działań rekonesansowych dotyczących Pałacu Kultury i Nauki w Warszawie.



Rys. 12. Fragment wyników dla zapytania dotyczącego wykorzystywania pakietu WordPress



Rys. 13. Strona wyników dla zapytania dotyczącego lokalizacji matrix.pkin.pl



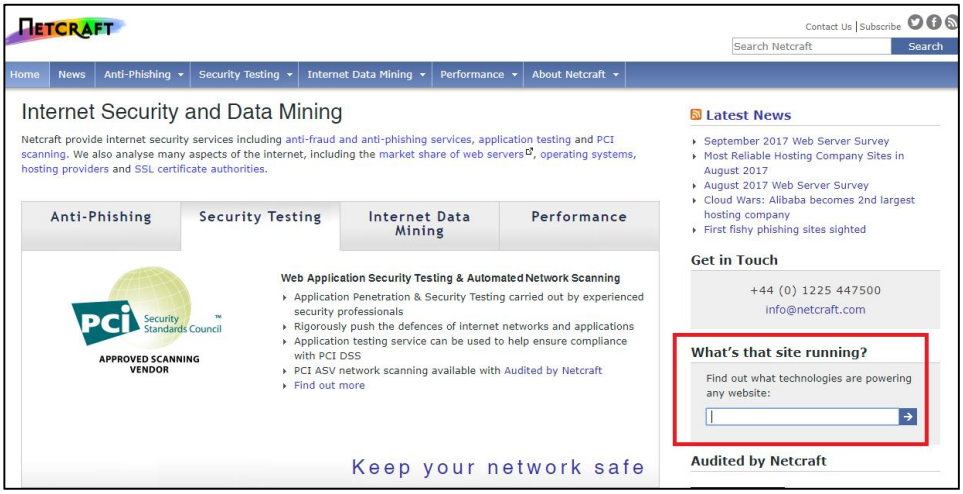
Rys. 14. Strona logowania do systemu pocztowego WebMail pod adresem matrix.pkin.pl

4.8. Narzędzie *NETCRAFTT*

Doskonałym narzędziem do pozyskiwania informacji jest NETCRAFT. Aby skorzystać z tego narzędzia należy odwiedzić stronę http://www.netcraft.com i zacząć poszukiwania w sekcji "*what's that site running?*" (rysunek 15). NETCRAFT zwróci adresy stron zawierających wyszukiwane słowa.

Jeśli którykolwiek z tych adresów nie został ujawniony podczas wcześniejszego wyszukiwania, to należy dodać go do kompletowanej listy domen lub adresów hostów związanych z badaną organizacją.

W trakcie opisywanego eksperymentu wspomniane narzędzie posłużyło przede wszystkim do pozyskiwania informacji odnośnie wykorzystywanych aktualnie platform systemowych i narzędziowych oraz stosowanych technologii. Uzyskiwano również informacje prezentujące historię zmian w zakresie stosowanych platform (historia hostingu). Przykłady pozyskanych danych przedstawiono na rysunkach 16 i 17.

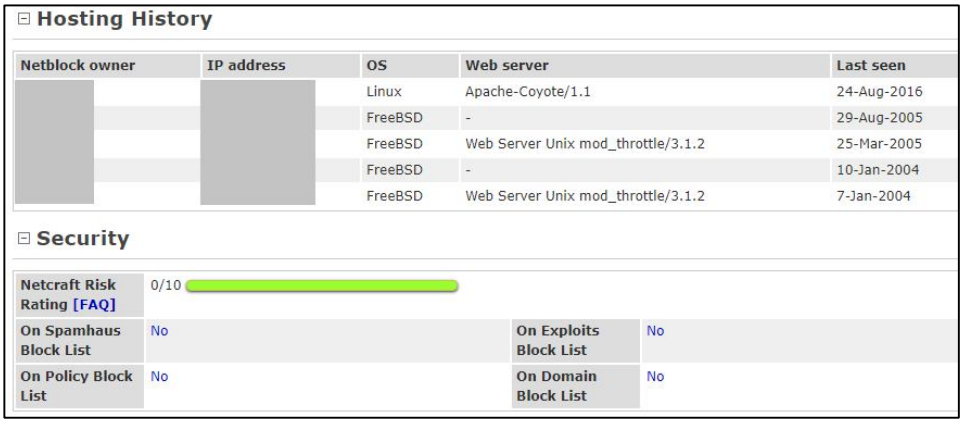


Rys. 15. Strona główna serwisu netcraft.com

4.9. Narzędzie THEHARVESTER

Program THEHARVESTER wyszukuje konta e-mail, nazwy użytkowników, nazwy hostów i subdomen. Jest to bardzo skuteczny skrypt w języku Python napisany przez Christiana Martorella. Pozwala skatalogować zarówno adresy e-mail jak i subdomeny, które są bezpośrednio związane

z zadanym celem. Gromadzi informacje z różnych źródeł publicznych. M.in.: Google, Google profles, Bing, PGP, LinkedIn, Yandex, People123, Jigsaw, Shodan.



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
		Linux	Apache-Coyote/1.1	24-Aug-2016
		FreeBSD	-	29-Aug-2005
		FreeBSD	Web Server Unix mod_throttle/3.1.2	25-Mar-2005
		FreeBSD	-	10-Jan-2004
		FreeBSD	Web Server Unix mod_throttle/3.1.2	7-Jan-2004

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

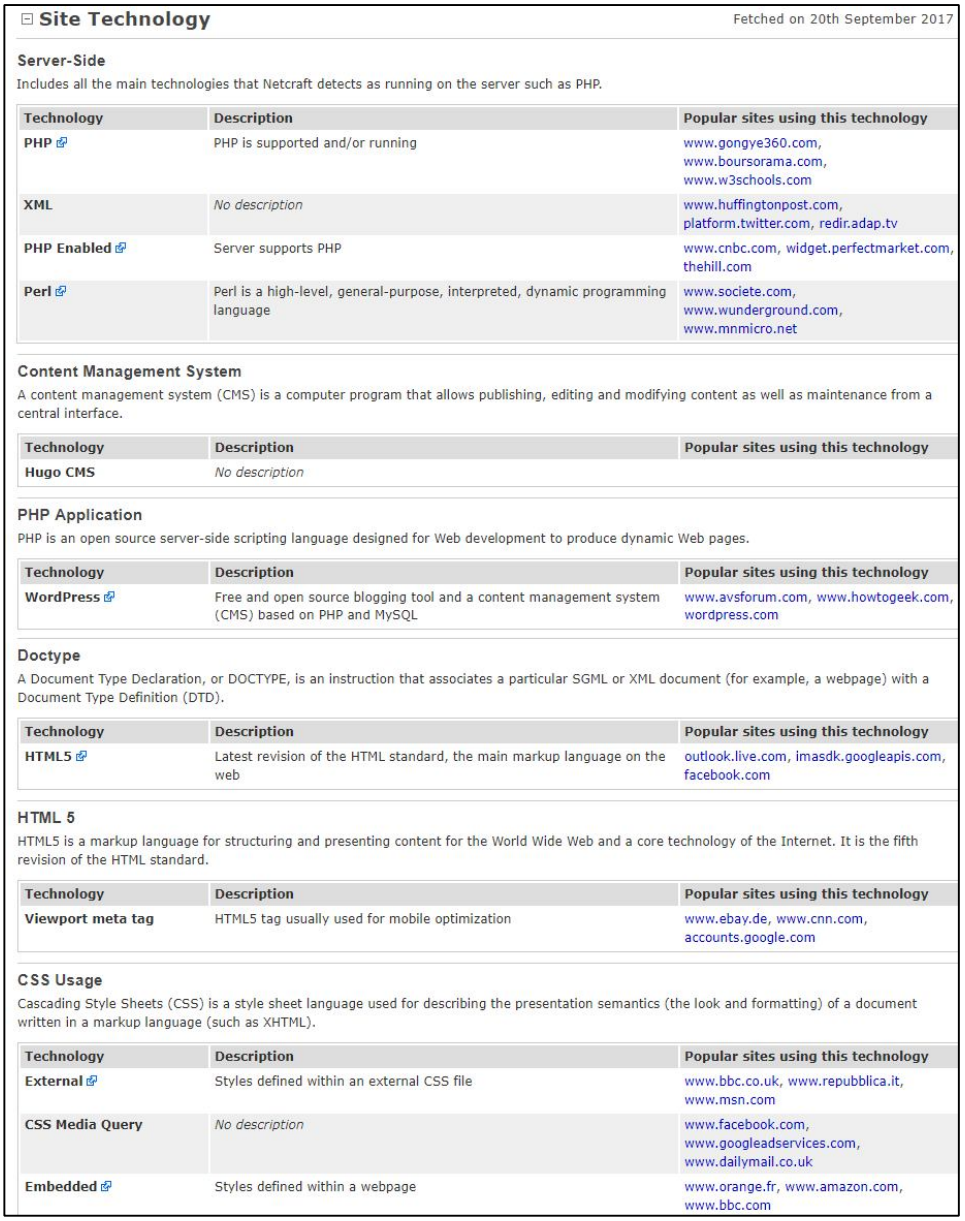
Rys. 16. Dane dotyczące historii hostingu i ogólnej oceny bezpieczeństwa uzyskane za pomocą serwisu netcraft.com

Chyba większość ludzi zakłada, że ich adres e-mail powinien być przyjazny dla właściciela i jego korespondentów. Wcześniej opisano już zagrożenia związane z zamieszczaniem na forach publicznych informacji przy użyciu firmowych adresów e-mail. Jednak istnieją dodatkowe zagrożenia, których wszyscy powinni być świadomi.

Jeżeli podczas rekonesansu wykryty zostanie adres e-mail pracownika z organizacji, którą interesuje się napastnik, to poprzez manipulowanie znakami przed symbolem "@", można utworzyć szereg potencjalnych nazw (aliasów) użytkowników w tej organizacji. Przykładowo, dość powszechnie stosowaną konwencją jest używanie dokładnie takiej samej nazwy użytkowników i adresów e-mail (przed symbolem "@"). Dysponując kilkoma potencjalnymi nazwami, można próbować metody ataku siłowego, w celu zdobycia dostępu do serwerów takich usług jak SSH, VPN lub FTP.

Tak jak poprzednio, znalezione nazwy domeny należy dodać do listy przeszukiwanych domen i ponownie rozpocząć proces rozpoznawczy. Pierwszy krok rekonesansu mający na celu ustalenie listy domen, które należy rozpoznać ma z natury charakter cykliczny, ponieważ dogłębne rozpoznanie często prowadzi do odkrycia nowych celów, co z kolei prowadzi do powtórzenia rekonesansu. W rezultacie, ilość czasu potrzebnego na zrealizowanie tego etapu może zmieniać się od kilku godzin do kilku tygodni. Należy pamiętać, że zdecydowany, złośliwy napastnik rozumie nie tylko moc dobrego zwiadu, ale także, że dysponuje często niemal nieograniczoną ilością czasu. Pentester

(zwłaszcza początkujący), powinien poświęcić na zbieranie informacji tyle czasu, ile to tylko jest możliwe.



Site Technology — Fetched on 20th September 2017

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.gongye360.com, www.boursorama.com, www.w3schools.com
XML	*No description*	www.huffingtonpost.com, platform.twitter.com, redir.adap.tv
PHP Enabled	Server supports PHP	www.cnbc.com, widget.perfectmarket.com, thehill.com
Perl	Perl is a high-level, general-purpose, interpreted, dynamic programming language	www.societe.com, www.wunderground.com, www.mnmicro.net

Content Management System

A content management system (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.

Technology	Description	Popular sites using this technology
Hugo CMS	*No description*	

PHP Application

PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description	Popular sites using this technology
WordPress	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL	www.avsforum.com, www.howtogeek.com, wordpress.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	outlook.live.com, imasdk.googleapis.com, facebook.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.ebay.de, www.cnn.com, accounts.google.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.bbc.co.uk, www.repubblica.it, www.msn.com
CSS Media Query	*No description*	www.facebook.com, www.googleadservices.com, www.dailymail.co.uk
Embedded	Styles defined within a webpage	www.orange.fr, www.amazon.com, www.bbc.com

Rys. 17. Dane dotyczące technologii stosowanych na jednej z badanych witryn

W trakcie opisywanego eksperymentu wielokrotnie wykorzystywane było również to narzędzie. Przykłady fragmentów pozyskanych danych dotyczących adresów mailowych, przedstawiono na rysunku 18.

4.10. Wyszukiwarki publiczne

Oprócz Google, dostępnych jest wiele wyszukiwarek publicznych, które umożliwiają przeszukanie ogólnie dostępnych zasobów internetowych. Należy do nich m.in. zaliczyć: SHODAN, DOMAINTOOLS, ALEXA, SERVERSNIFF, CENTRALOPS, ROBTEX, PIPL YONAME. Należy jednak zwrócić uwagę, że część funkcjonalności dostarczanej przez te narzędzia może wykraczać poza granice rekonesansu pasywnego. Tak jest np. w przypadku serwisów CENTRALOPS czy ROBTEX.

Niektóre z wymienionych były testowane w trakcie opisywanego eksperymentu. Na rysunku 19 przedstawiono fragment danych uzyskanych za pomocą serwisu SHODAN. Ta wyszukiwarka jest wyspecjalizowana w indeksowania informacji zawartych w banerach obsługiwanych przez urządzenia podłączone do Internetu. Wyszukiwarka głównie indeksuje „znaleziska" z portu 80, ale także niektóre banery serwerów Telnet, SSH i FTP.

4.11. Rekonesans dotyczący DNS

Wartościowe dane można uzyskać podczas rekonesansu z systemu DNS. Rozpoznawanie DNS jest uważane za rekonesans aktywny ze względu na fakt, że wymaga interakcji z maszynami będącymi w posiadaniu cennych informacji. Nie jest to jednak prawdą, gdyż kontakt z serwerami DNS domeny badanej nie musi być bezpośredni. Uzyskiwane dane mogą pochodzić z innych serwerów niż serwery DNS domeny badanej, czyli z serwerów nieautorytatywnych dla danej domeny Mogły być one pozyskane przez te serwery, zanim rozpoczął się rekonesans, lub w wyniku działań podejmowanych w czasie rekonesansu.

Informacje mogą pochodzić z rekordów zasobów:

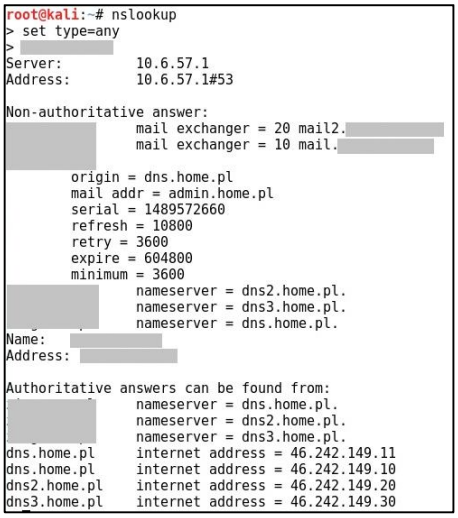
- CNAME – określa tzw. aliasy nazwowe. Host o określonym adresie może występować pod kilkoma nazwami;
- A – określa odwzorowanie nazwy domenowej w adres IP. Czasem może zawierać jeszcze inną przydatną informację;
- MX – określa nazwy przypisane do serwerów pocztowych;
- SRV – określa lokalizacjęi usług.

Rys. 18. Fragment danych pozyskanych za pomocą programu *theharvester*

Rys. 19. Dane dotyczące wykorzystywanego serwera uzyskane za pomocą serwisu SHODAN

Program *nslookup* jest narzędziem, które służy do odpytywania dowolnych serwerów nazw o konkretne zapisy. Chociaż nie jest on najbardziej skutecznym narzędziem DNS w testach, to jednak jest to narzędzie które jest dostępne niemalże w każdym systemie operacyjnym. Program *nslookup* jest narzędziem typu cross-platform i jest preinstalowany na większości systemów operacyjnych.

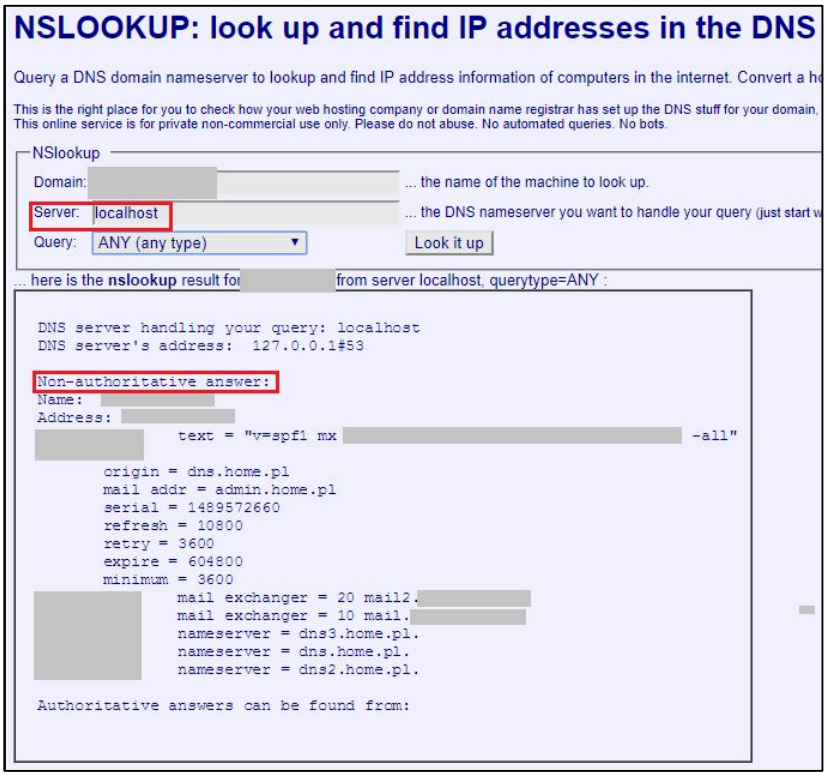
Ponieważ można go uruchomić z jednego wiersza polecenia, łatwo jest utworzyć skrypt, który automatyzuje zadanie pozyskiwania informacji o wielu domenach lub hostach i zapisuje wynik do pliku tekstowego.



Rys. 20. Dane uzyskane za pomocą programu nslookup z nieautorytatywnego serwera DNS

Narzędziem alternatywnym w stosunku do programu *nslookup* jest *dig*. Oprócz tego w Internecie dostępnych jest wiele witryn, które umożliwiają pozyskiwanie informacji z systemu DNS. Należy jednak zwrócić uwagę, że niektóre z nich wychodzą poza ramy rekonesansu pasywnego i wobec tego nie należy z nich korzystać.

Na rysunku 20 przedstawiono obraz uzyskany podczas pozyskiwania danych z systemu DNS dla jednej z domen testowanych podczas eksperymentu. Jak można zauważyć odpowiedź nie jest autorytatywna, tzn. danych nie pozyskano z żadnego autorytatywnego serwera DNS badanej domeny. Spełniony został w ten sposób warunek rekonesansu pasywnego. Podobnie jest w przypadku raportu przedstawionego na rysunku 21. Uzyskano go dzięki wykorzystaniu internetowej witryny narzędziowej kloth.net. Ponieważ odpytywany serwer DNS (pole zaznaczone ramką) nie jest serwerem autorytatywnym dla badanej domeny, więc uzyskana odpowiedź nie jest autorytatywna. W tym przypadku również został spełniony warunek rekonesansu pasywnego.



Rys. 21. Dane uzyskane za pomocą witryny kloth.net z nieautorytatywnego serwera DNS

5. Podsumowanie

Przeprowadzony eksperyment pozwolił wykazać, że metody i narzędzia rekonesansu pasywnego, które stosowane były kilka a nawet kilkanaście lat temu, w dalszym ciągu mogą być skuteczne. Prowadzi to do niezbyt optymistycznego wniosku, że tzw. świadomość zagrożeń w dalszym ciągu jest dość niska. Jak najbardziej uzasadnione są wobec tego prace badawcze oraz działania edukacyjne w tym zakresie, co jest m.in. realizowane w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki Wojskowej Akademii Technicznej.

Przeprowadzony eksperyment nie wyczerpuje metod i narzędzi, które mogą być wykorzystywane w czasie fazy pasywnego rekonesansu testów penetracyjnych. Z tych względów będzie on kontynuowany. Będzie on też dotyczył innych domen niż te, które zostały przebadane w pierwszej edycji. Oprócz powtórzenia działań, które zrealizowano podczas pierwszej edycji

i opisano w niniejszym artykule, należałoby uwzględnić lub pogłębić uzyskiwanie informacji na podstawie danych pozyskiwanych przykładowo z:

- grup dyskusyjnych,
- witryn partnerów biznesowych,
- publicznych wyszukiwarek.

Celem kolejnego etapu badań dotyczących pasywnego rekonesansu będzie również rozszerzenie listy narzędzi, które można by było zastosować. Jeżeli wyniki będą interesujące, to zostaną przedstawione w kolejnym artykule.

Literatura

[1] WHITAKER A., NEWMAN D.P., *Penetration Testing and Network Defense*. Cisco Press, Indianapolis, 2006.

[2] BEAVER K, *Hacking for Dummies.* Wiley Publishing Inc, Hoboken, 2015.

[3] ALLEN L., *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*. Packt Publishing Ltd, Birmingham, 2012.

[4] WILHELM T., *Professional Penetration Testing - Creating and Operating a Formal Hacking Lab*. Syngress Elsevier, New York, 2013.

[5] ENGEBRETSON P., *The Basics of Hacking and Penetration Testing*. Syngress Elsevier, New York, 2013.

[6] BALOCH R., *Ethical Hacking and Penetration Testing Guide*. CRC Press, Boca Raton, 2015.

[7] ALLEN L., HERIYANTO T., ALI S., *Kali Linux – Assuring Security by Penetration Testing*. Packt Publishing Ltd, Birmingham, 2014.

[8] GRAVES K., *CEH – Certified Ethical Hacker – Study Gu*ide. Wiley Publishing Inc, Indianapolis, 2010.

[9] KENNEDY D., O'GORMAN J., KEARNS D., AHARONI M., *Metasploit – The Penetration Tester Guide*. No Starch Press, San Francisco, 2011.

[10] MCCLURE S., SCAMBRAY J., KURTZ G., *Hacking Exposed - Network Security Secrets and Solutions*. Mc Graw Hill, New York, 2012.

[11] PALE P.C., *Nmap 6: Network Exploration and Security Auditing Cookbook*. Packt Publishing Ltd, Birmingham, 2012

[12] AGARVAL M., SINGH A, *Metasploit Penetration Testing Cookbook*. Packt Publishing Ltd, Birmingham, 2013.

[13] WEIDMAN G., *Penetration Testing – A Hands-On Introduction to Hacking*. No Starch Press, San Francisco, 2014.

[14] KIM P., *The Hacker Playbook 2: Practical Guide to Penetration Testing.* Secure Planet, North Charleston, 2015.

[15] HERTZOG R., O'GORMAN J., AHARONI M., *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. OffSec Press, Cornelius, 2017.

[16] PROWSE D.L., *CompTIA Security+ Deluxe Cert Guide (SY0-401)*. Wiley Publishing, Indianapolis, 2015.

[17] LONG J., GARDNER B., BROWN J., *Google Hacking for Penetration testers*. Syngress Elsevier, Waltham, 2016.

Passive reconnaissance in penetration tests

ABSTRACT: The paper describes general principles of conducting penetration tests. The focus is primarily on a passive reconnaissance phase. Methods and tools used during such a reconnaissance are described. Some research results have been presented to verify the validity of some methods and tools.

KEYWORDS: security, penetration test, reconnaissance

Praca wpłynęła do redakcji: 22.09.2017 r.