Zeszyty Naukowe WWSI, No 17, Vol. 11, 2017, s. 69-87
DOI: 10.26348/znwwsi.17.69

Analiza wybranych narzędzi do pozyskiwania informacji o zaatakowanym systemie informatycznym

Dariusz Chaładyniak*, Andrzej Czarnecki†

Warszawska Wyższa Szkoła Informatyki

Abstrakt

Rekonesans jest pierwszym etapem w procesie przeprowadzenia testów penetracyjnych, polegający na zbieraniu informacji o celu ataku z ogólnie dostępnych zewnętrznych źródeł. Zebrane dane można wykorzystać w celu pozyskania np.: danych osobowych pracowników, adresów e-mail, nazw domen, adresów IP systemów osiągalnych przez sieć Internet. Dodatkowo można uzyskać informację o usługach TCP (*ang. Transmission Control Protocol*) i UDP (*ang. User Datagram Protocol*), typach systemów wykrywania włamań IPS (*ang. Intrusion Prevention System*) oraz IDS (*ang. Intrusion Detection System*).

Rekonesans powinien być wykonany metodą pasywną, podczas której jest mniejsze ryzyko wykrycia działalności atakującego. Ponadto jest to legalne wyszukiwanie informacji dostępnych w Internecie. Metoda ta umożliwia zbieranie informacji bez ujawniania, że jakiekolwiek czynności są prowadzone. Dzięki użyciu wybranych programów do przeprowadzania rekonesansu, przeanalizowano dużo informacji o badanej firmie.

Słowa kluczowe – rekonesans, protokoły sieciowe, adresy IP, systemy DNS, usługi sieciowe

* E-mail: dchalad@wwsi.edu.pl
† E-mail: a_czarnecki@poczta.wwsi.edu.pl

Zgłoszono do druku 21 października 2017 r.

1. Wprowadzenie

Osoby przeprowadzające testy bezpieczeństwa systemów informatycznych wspomagają się specjalistycznym oprogramowaniem, które znacząco ułatwia i przyśpiesza wykonywane czynności. Bardzo ważne jest użycie odpowiednich narzędzi w określonych etapach, aby uzyskać spodziewane efekty i otrzymać zadowalające wyniki. Rekonesans jest etapem, w trakcie którego jest zdobywana wiedza o badanej firmie z ogólnie dostępnych źródeł w Internecie. Zdobyte informacje zawierające nazwy i adresy IP serwerów, listę nazw użytkowników z ich adresami e-mailowymi oraz wyciągnięte dokumenty mogą posłużyć do przygotowania kierunków ataku.

2. Analiza oprogramowania do pozyskiwania informacji o zaatakowanym systemie informatycznym firmy

W procesie analizy pozyskanych informacji w wyniku przeprowadzonego rekonesansu można wykorzystać poniższe narzędzia programistyczne.

2.1. Wyszukiwarka Google

Wykorzystanie specjalnych możliwości wyszukiwarki Google umożliwia dokładne znalezienie interesujących nas danych. Zaawansowane algorytmy tej wyszukiwarki pomagają w odszukaniu informacji przydatnych z punktu widzenia analizy bezpieczeństwa. Dzięki odpowiednim zapytaniom można uzyskać dostęp do urządzeń firmowych na przykład kamer VOIP (*ang. Voice over Internet Protocol*), plików konfiguracyjnych serwera i aplikacji, które nie powinny być ujawnione, plików z hasłami zapisanymi jawnym tekstem, prywatnych plików użytkowników i wiele innych danych.

Dzięki użyciu fraz (*ang. google dorks*) można zawęzić liczbę stron umieszczanych w wyniku wyszukiwania co znacząco skraca czas poszukiwań. Wszystkie opcje, które można użyć w wyszukiwarce **Google** dostępne są na stronie *http://www.googlehacking.com.pl*.

Lista przykładowych zapytań:

site:wp.pl Dariusz Kowalski – polecenie **site** umożliwia znalezienie wszystkich informacji o Panu Kowalskim w domenie wp.pl;

intitle:Dariusz Kowalski – zapytanie powoduje umieszczenie wyniku wyszukiwania stron internetowych, które zawierają przynajmniej jedno ze słów: **Dariusz** lub **Kowalski**;

allintitle:Dariusz Kowalski – dyrektywa, która umieszcza w wyniku wyszukiwania tylko te strony internetowe, które w tytule zawierają wszystkie frazy: **Dariusz** i **Kowalski** wymienione w wyrażeniu wyszukiwania;

allintitle:index of – wyrażenie wyświetla listę wszystkich katalogów, które zostały zindeksowane i są dostępne na serwerze WWW. Na przykład **allintitle of hacking** – wyświetli wszystkie katalogi z **hackingiem;**

inurl:Dariusz Kowalski – dyrektywa, która wyświetli strony internetowe zawierające określone słowa w adresie URL (*ang. Uniform Resource Locator*);

cache:Dariusz Kowalski – wyrażenie umożliwia przeszukanie bufora wyszukiwarki Google, gdzie mogą znajdować się materiały już usunięte z Internetu;

filetype:pdf – uzyskanie wyniku zawierającego tylko dokumenty PDF;

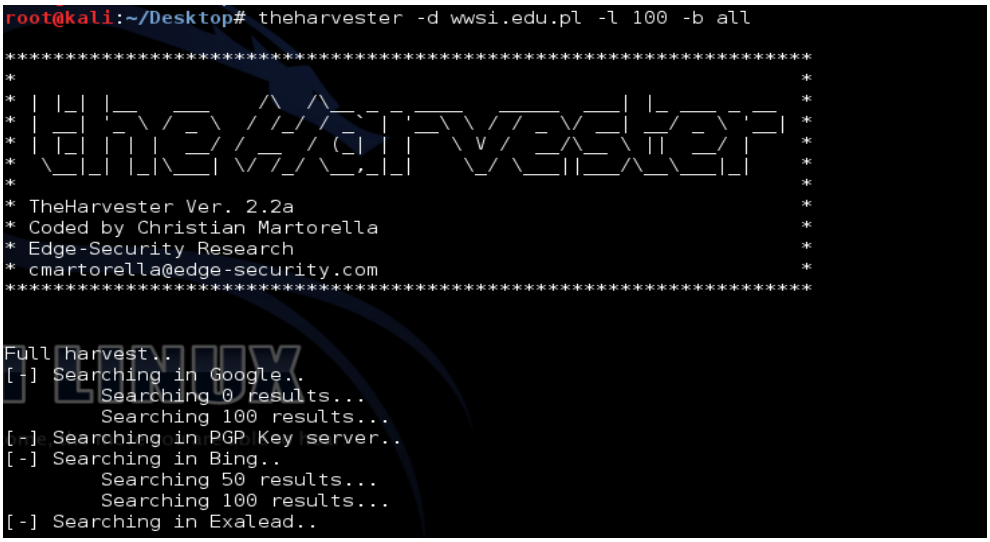
site:wp.pl filetype:pdf – przez połączenie dyrektyw można zwiększyć wyszukiwanie. W tym połączeniu chcemy wyszukać wszystkie dokumenty PDF dostępne w witrynie internetowej wp.pl.

Narzędzie to szybko wyszukuje informacje z całego świata, a przy tym cechuje się ogólnodostępnością i co najważniejsze jest bezpłatne.

2.2. theHarvester

theHarvester [1] to bardzo efektywny skrypt służący do wyszukiwania i katalogowania nazw użytkowników w Internecie poprzez zbieranie adresów e-mail oraz subdomen bezpośrednio powiązanych z testowaną organizacją. Informacje o adresach znajdowane są w bardzo różnych źródłach, takich jak Google, Linkedln, PGP, Facebook i wielu innych portalach społecznościowych.

Do przeprowadzenia analizy została użyta strona Warszawskiej Wyższej Szkoły Informatyki (patrz rysunek 1).



Rysunek 1. Uruchomienie narzędzia theHarvester

Opis poleceń:

- **d** – opcja wskazująca domenę;
- **l** – opcja powodująca ograniczenie liczby danych umieszczonych w wyniku działania narzędzia;
- **b** – opcja wskazująca na publiczne repozytoria, które mają zostać przeszukane (w tym przypadku wszystkie).

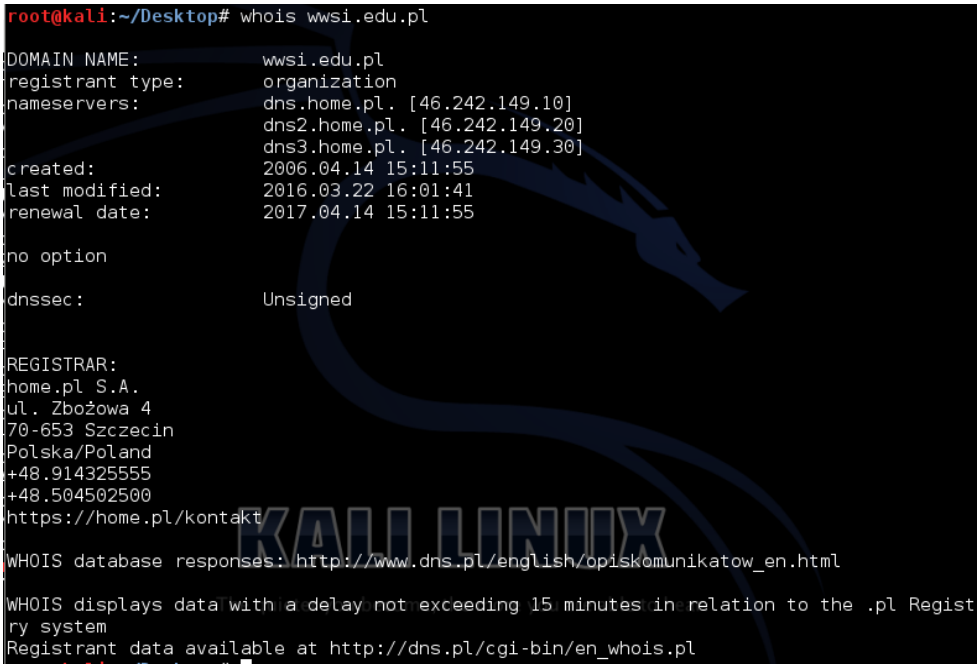
Jest to bardzo przydatne narzędzie, dzięki któremu można pozyskać adresy poczty elektronicznej osób zatrudnionych lub powiązanych bezpośrednio z firmą, w której wykonywane są testy penetracyjne (patrz rysunek 2). Uzyskane informacje doskonale nadają się do wykorzystania w atakach socjotechnicznych.

```
[+] Emails found:
---------------
w_wozniak@wwsi.edu.pl
p_kordys@poczta.wwsi.edu.pl
dziekanat@wwsi.edu.pl
mprzybysz@wwsi.edu.pl
rektorat@wwsi.edu.pl
rekrutacja@wwsi.edu.pl

[+] Hosts found in search engines:
------------------------------------
148.81.195.152:poczta.wwsi.edu.pl
148.81.195.146:www.wwsi.edu.pl
148.81.195.146:student.wwsi.edu.pl
148.81.195.134:www.studenci.wwsi.edu.pl
148.81.195.146:praca.wwsi.edu.pl
148.81.195.156:rekrutacja.wwsi.edu.pl
148.81.195.152:poczta.wwsi.edu.pl
148.81.195.146:projektyefs.wwsi.edu.pl
148.81.195.146:aptaszni.wwsi.edu.pl
148.81.195.137:podyplomowe.wwsi.edu.pl
148.81.195.146:kibr.wwsi.edu.pl
148.81.195.146:core-it.wwsi.edu.pl
148.81.195.134:www.techor.wwsi.edu.pl
148.81.195.134:techor.wwsi.edu.pl
148.81.195.146:www.abit.wwsi.edu.pl
148.81.195.146:wlf-info-platforma.wwsi.edu.pl
148.81.195.146:zeszyty-naukowe.wwsi.edu.pl
148.81.195.146:www.konferencjabi.wwsi.edu.pl
[+] Virtual hosts:
==================
148.81.195.152l  poczta.wwsi.edu.pl
148.81.195.146l  www.wwsi.edu.pl
148.81.195.146l  student.wwsi.edu.pl
148.81.195.146l  core-it.wwsi.edu.pl
148.81.195.146l  pwi.edu.pl
148.81.195.146l  zeszyty-naukowe.wwsi.edu.pl
148.81.195.146l  uniwersytet-wirtualny.edu.pl
148.81.195.146l  efektywni50plus.wwsi.edu.pl
148.81.195.146l  www.ptnei.pl
148.81.195.146l  kibr.wwsi.edu.pl
148.81.195.146l  aptaszni.wwsi.edu.pl
148.81.195.146l  www.informatykaplus.edu.pl
```

Rysunek 2. Wyniki działania programu theHarvester

2.3. Whois

Usługa Whois [2] dostarcza danych o właścicielu domeny, nazwach serwerów DNS, adresach IP oraz informacjach kontaktowych. Materiały są dostępne publicznie z bazy danych Naukowej i Akademickiej Sieci Komputerowej (NASK). Zgodnie z prawem o ochronie danych osobowych nie powinna zawierać danych osób fizycznych. W systemie Kali Linux jest wbudowany protokół Whois, który na podstawie nazwy domeny wyświetli wszystkie informacje jakie zostały podane w trakcie rejestracji (patrz rysunek 3).

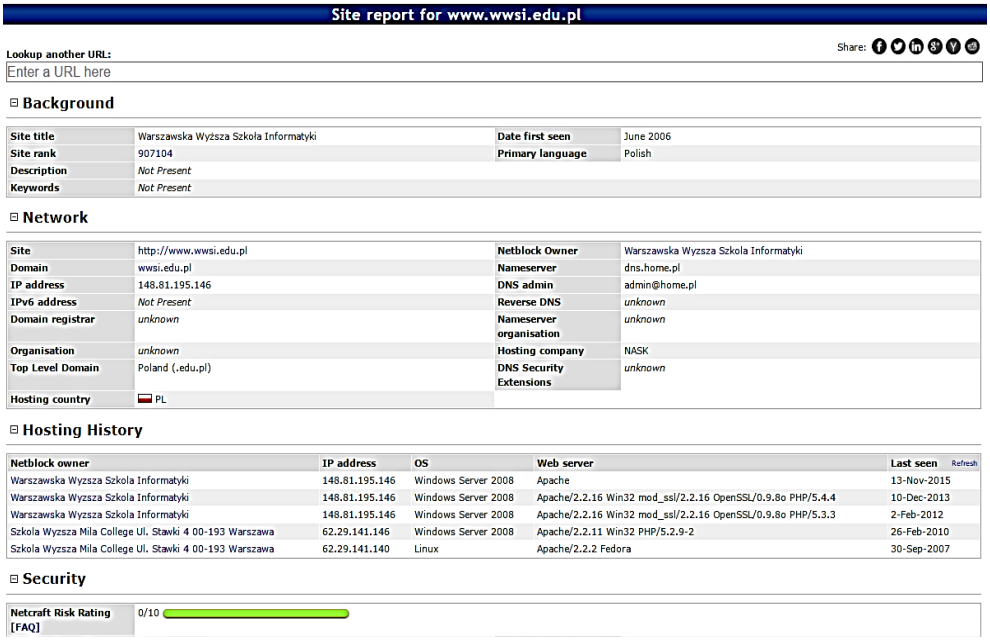


Rysunek 3. Polecenie Whois zbierające dane z witryny

Baza usług Whois jest również dostępna przez przeglądarkę internetową a uzyskane dane są identyczne jak te za pomocą narzędzia w Kali Linux. Jeżeli serwery DNS są wyświetlone jedynie w postaci nazw, to należy użyć polecenie Host**,** aby przekształcić je na adresy IP.

2.4. Netcraft

Netcraft [3] jest to serwis dostarczający informacji na temat interesującej nas witryny w postaci raportu, z którego możemy otrzymać szczegółowe dane o oprogramowaniu, jakie jest wykorzystywane przez serwery WWW i DNS, adresy IP i wiele innych usług wykorzystywanych w badanej firmie (patrz rysunek 4).



Site report for www.wwsi.edu.pl

Lookup another URL:
Enter a URL here

Share:

Background

Site title	Warszawska Wyższa Szkoła Informatyki	**Date first seen**	June 2006
Site rank	907104	**Primary language**	Polish
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://www.wwsi.edu.pl	**Netblock Owner**	Warszawska Wyższa Szkoła Informatyki
Domain	wwsi.edu.pl	**Nameserver**	dns.home.pl
IP address	148.81.195.146	**DNS admin**	admin@home.pl
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	NASK
Top Level Domain	Poland (.edu.pl)	**DNS Security Extensions**	*unknown*
Hosting country	PL		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Warszawska Wyższa Szkoła Informatyki	148.81.195.146	Windows Server 2008	Apache	13-Nov-2015
Warszawska Wyższa Szkoła Informatyki	148.81.195.146	Windows Server 2008	Apache/2.2.16 Win32 mod_ssl/2.2.16 OpenSSL/0.9.8o PHP/5.4.4	10-Dec-2013
Warszawska Wyższa Szkoła Informatyki	148.81.195.146	Windows Server 2008	Apache/2.2.16 Win32 mod_ssl/2.2.16 OpenSSL/0.9.8o PHP/5.3.3	2-Feb-2012
Szkoła Wyższa Mila College Ul. Stawki 4 00-193 Warszawa	62.29.141.146	Windows Server 2008	Apache/2.2.11 Win32 PHP/5.2.9-2	26-Feb-2010
Szkoła Wyższa Mila College Ul. Stawki 4 00-193 Warszawa	62.29.141.140	Linux	Apache/2.2.2 Fedora	30-Sep-2007

Security

Netcraft Risk Rating [FAQ]	0/10

Rysunek 4. Przykład informacji zdobytych za pomocą serwisu Netcraft

Informacje uzyskane pozwalają już na samym początku określić systemy operacyjne i numery wersji, jakie są używane w danej organizacji. Ciekawe jak zareagowałby administrator, jeżeli otrzymałby spreparowanego e-maila z firmy NASK z prośbą o zalogowanie się i sprawdzenie zabezpieczeń. Serwis Netcraft znacznie ułatwia i przyśpiesza pozyskiwanie informacji na temat badanej firmy w Internecie.

2.5. Nslookup

Aplikacja Nslookup [4] jest przeznaczona do wykonywania zapytań do serwera DNS w celu uzyskania szczegółowych informacji o nim. Pozwala na znajdywanie adresów serwerów pocztowych, serwerów domenowych i komputerów w sieci. Umożliwia pracę w trybie nieinteraktywnym wpisując polecenie ***nslookup*** i nazwę domeny oraz interaktywnym poprzez uruchomienie programu i korzystanie z argumentów (patrz rysunek 5).

Rysunek 5. Wyniki działania narzędzia Nslookup w trybie interaktywnym

Opis poleceń:

man nslookup – dokumentacja narzędzia nslookup;

>set type=SOA – rekord SOA (*ang. Start of Authority*) wyświetla informacje o ustawieniach serwera;

>set type=NS – rekord NS (*ang. Name Server*) wyświetla nazwy serwerów DNS dla danej domeny;

>set type=MX – rekord MX (*ang. Mail Exchanger*) wyświetla nazwę serwera poczty elektronicznej.

Za pomocą użytych zapytań zostało zebranych wiele dokładnych informacji o ustawieniach serwera DNS oraz adres serwera pocztowego przeglądanej witryny poprzez przeszukiwanie rekordów **MX**. Ponieważ poczta przesyłana i odbierana nie

może być blokowana przez routery i zapory sieciowe, dlatego też ustalenie adresu serwera pocztowego umożliwi dostanie się do wewnętrznej sieci. Uzyskane nazwy serwerów można za pomocą narzędzia Host zamienić na adresy IP.

2.6. Dig

Dobrą alternatywą programu Nslookup jest aplikacja Dig (*ang. Domain Internet Groper*) [5] przeznaczona do wyciągania wielu rekordów informacji z serwera DNS. Jest to wszechstronne narzędzie, które potrafi zwrócić niemal każdą informację, do jakiej ma dostęp odpytywany serwer. Dostarcza obszernych informacji diagnostycznych oraz pozwala zdiagnozować ile czasu potrzeba komputerowi na uzyskanie adresu IP dla nazwy domeny. Jest standardowo w dystrybucjach Linuxa jak i Unixa, ale również może być instalowany w systemie operacyjnym Windows.

Za pomocą programu Dig są dostępne pełne informacje o ustawieniach serwera z rekordu SOA (patrz rysunek 6). Rekord NS pokazuje jakie nazwy serwerów DNS są przypisane do domeny (patrz rysunek 7). Natomiast rekord MX przedstawia nazwę serwera poczty elektronicznej (patrz rysunek 8).

```
root@kali:~/Desktop# dig wwsi.edu.pl -t SOA

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> wwsi.edu.pl -t SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65194
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;wwsi.edu.pl.                   IN      SOA

;; ANSWER SECTION:
wwsi.edu.pl.            5       IN      SOA     dns.home.pl. admin.home.pl. 1458658902
10800 3600 604800 3600

;; Query time: 18 msec
;; SERVER: 192.168.216.2#53(192.168.216.2)
;; WHEN: Tue Sep  6 06:52:29 2016
;; MSG SIZE  rcvd: 80
```

Rysunek 6. Pozyskane informacje z rekordu SOA

```
root@kali:~/Desktop# dig wwsi.edu.pl -t NS

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> wwsi.edu.pl -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19921
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;wwsi.edu.pl.                   IN      NS

;; ANSWER SECTION:
wwsi.edu.pl.            5       IN      NS      dns3.home.pl.
wwsi.edu.pl.            5       IN      NS      dns.home.pl.
wwsi.edu.pl.            5       IN      NS      dns2.home.pl.

;; Query time: 21 msec
;; SERVER: 192.168.216.2#53(192.168.216.2)
;; WHEN: Tue Sep  6 06:52:22 2016
;; MSG SIZE  rcvd: 90
```

Rysunek 7. Pozyskane informacje z rekordu NS

```
root@kali:~/Desktop# dig wwsi.edu.pl -t MX

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> wwsi.edu.pl -t MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2959
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;wwsi.edu.pl.                   IN      MX

;; ANSWER SECTION:
wwsi.edu.pl.            5       IN      MX      10 barracuda.wwsi.edu.pl.

;; Query time: 28 msec
;; SERVER: 192.168.216.2#53(192.168.216.2)
;; WHEN: Tue Sep  6 06:52:15 2016
;; MSG SIZE  rcvd: 55
```

Rysunek 8. Pozyskane informacje z rekordu MX

2.7. Host

Za pomocą programu Host [6] można przyporządkować nazwy serwerów do ich adresów IP (patrz rysunek 9).

```
root@kali:~/Desktop# host dns2.home.pl
dns2.home.pl has address 46.242.149.20
dns2.home.pl has address 46.242.149.21
dns2.home.pl has IPv6 address 2a02:25a8:1::20
dns2.home.pl has IPv6 address 2a02:25a8:1::21
root@kali:~/Desktop# host dns3.home.pl
dns3.home.pl has address 46.242.149.31
dns3.home.pl has address 46.242.149.30
dns3.home.pl has IPv6 address 2a02:25a8:1::31
dns3.home.pl has IPv6 address 2a02:25a8:1::30
root@kali:~/Desktop# host dns.home.pl
dns.home.pl has address 46.242.149.10
dns.home.pl has address 46.242.149.11
dns.home.pl has IPv6 address 2a02:25a8:1::11
dns.home.pl has IPv6 address 2a02:25a8:1::10
root@kali:~/Desktop# host barracuda.wwsi.edu.pl
barracuda.wwsi.edu.pl has address 148.81.195.133
root@kali:~/Desktop#
```

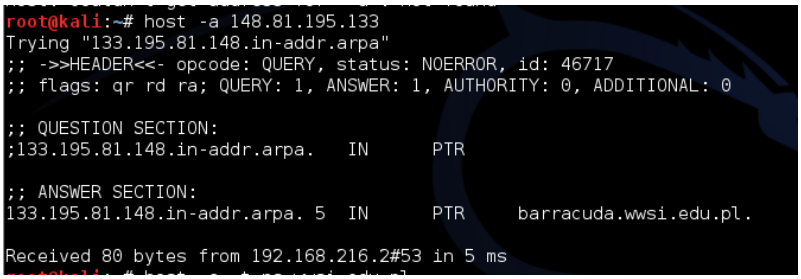
Rysunek 9. Przykład odwzorowania nazw domenowych na adresy IP

Narzędzie umożliwia również uzyskanie listy rekordów serwerów DNS i serwerów pocztowych obsługujących testowaną organizację (patrz rysunek 10).

```
root@kali:~# host -a wwsi.edu.pl
Trying "wwsi.edu.pl"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48398
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;wwsi.edu.pl.                   IN      ANY

;; ANSWER SECTION:
wwsi.edu.pl.            5       IN      MX      10 barracuda.wwsi.edu.pl.
wwsi.edu.pl.            5       IN      A       148.81.195.146
wwsi.edu.pl.            5       IN      SOA     dns.home.pl. admin.home.pl. 1458
658902 10800 3600 604800 3600
wwsi.edu.pl.            5       IN      NS      dns.home.pl.
wwsi.edu.pl.            5       IN      NS      dns2.home.pl.
wwsi.edu.pl.            5       IN      NS      dns3.home.pl.

Received 174 bytes from 192.168.216.2#53 in 125 ms
```

Rysunek 10. Przykład wykazu serwerów DNS

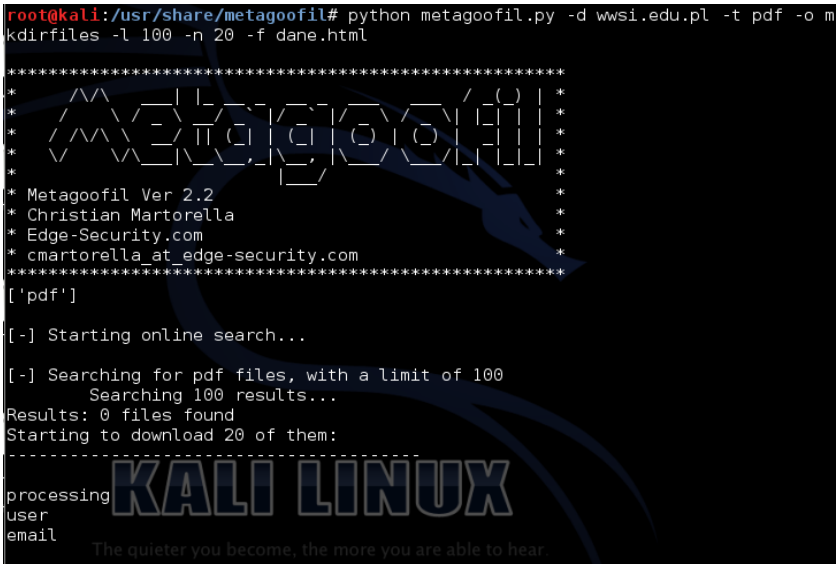
Można również wykorzystać ten program w celu przeprowadzenia konwersacji w drugą stronę, czyli przekształcenia adresu IP w nazwę komputera/serwera (patrz rysunek 11).



Rysunek 11. Przykład pozyskania nazwy z adresu IP

2.8. Metagoofil

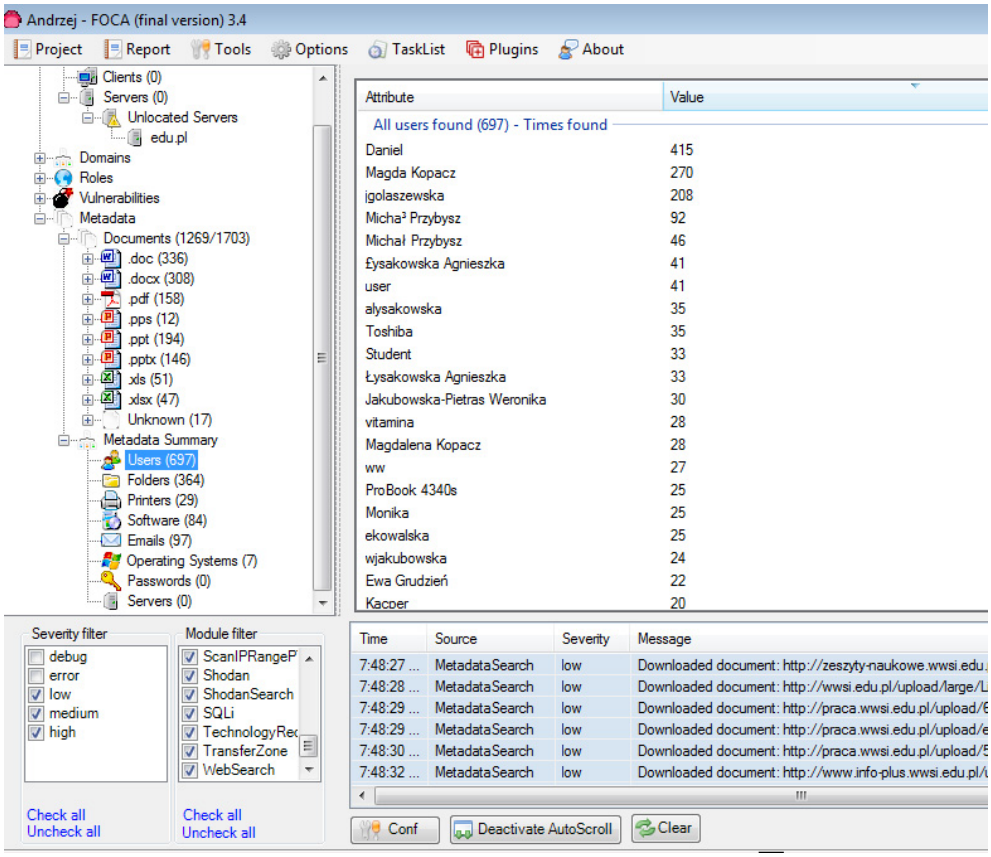
Narzędzie MGF (*ang. Metagoofil*) [7] służy do wyodrębnienia metadanych, czyli danych o danych. Na przykład podczas tworzenia dokumentu w Microsoft Word wraz z utworzonym plikiem zostają zapisane informacje, zwierające między innymi nazwę pliku, jego wielkość, właściciela, ścieżkę prowadzącą do lokalizacji, wersję oprogramowania. Dzięki temu programowi możemy odkryć dodatkowo nazwę użytkownika i jego adres IP. Narzędzie to wyszukuje informacje i przedstawia w bardzo czytelnym raporcie, który można przejrzeć przez przeglądarkę. Pobrane dokumenty mogą zawierać interesujące dane, które można wykorzystane w późniejszych etapach przeprowadzanych testów penetracyjnych.



Rysunek 12. Przykład działania programu Megagoofil

2.9. FOCA

FOCA (*ang. Fingerprinting Organizations with Collected Archives*) [8] jest narzędziem, które podobnie jak Metagoofil jest używane do wykonywania audytów bezpieczeństwa w celu wyszukiwania metadanych zawartych w wykonanych dokumentach dostępnych przez przeglądarkę. Program poprzez wyszukiwarkę internetową odnajduje materiały dotyczące testowanej organizacji. Wyszukane dokumenty program zapisuje na dysku i przeprowadza analizę pod kątem określonych kategorii, w celu pozyskania cennych informacji z punktu widzenia bezpieczeństwa.



Rysunek 13. Efekt działania narzędzia FOCA

Jak widać na rysunku nr 13, program zadziałał poprawnie i w domenie *wwsi.edu.pl* znalazł wszystkie zaznaczone rodzaje dokumentów. Zebrane materiały zostały przeskanowane w celu wyszukania specjalnych danych, które zostały zindeksowane z podziałem na kategorie zawierające nazwy użytkowników, drukarek, systemów operacyjnych w jakim zostały utworzone, adresów pocztowych, wersji oprogramowania użytego do wykonania dokumentu oraz haseł.

Możliwości programu są naprawdę rewelacyjne i uzyskane efekty mogą zaskoczyć. Administratorzy powinni bardzo często używać tego narzędzia aby uniknąć problemów polegających na pozostawieniu jakiegoś ważnego dokumentu zawierającego na przykład hasła. FOCA wykonuje całą pracę automatycznie i w bardzo przejrzystej formie przedstawia zgromadzone wyniki, które potem można ująć w końcowym raporcie.

2.10. Discover Script

Za pomocą frameworka analitycznego Discover Scripts [9] jest możliwe automatyczne wykonanie wszystkich czynności. Można zebrać informacje o nazwie domeny, adresów IP, adresów e-mailowych, informacje z Whois i wiele innych. Wyniki zebrane są wyświetlane przez przeglądarkę.

Character Omission	wsi.edu.pl	91.200.38.106	Poland	mail.wsi.edu.pl	pl
Character Omission	wws.edu.pl	185.36.168.127		wws.edu.pl	pl
Character Omission	wwsi.ed.pl	178.63.56.210	Germany	pinkmail.adpilot.co	pl
Character Omission	wwsi.eu.pl	89.161.155.85	Poland	eu.pl	pl
Character Swap	wws.iedu.pl	194.29.153.17	Poland		pl
Character Swap	wwsi.deu.pl	212.91.7.33	Poland		pl
Character Replacement	wwsi.edy.pl	37.187.91.221	Austria		pl
Character Replacement	wwsi.efu.pl	212.91.7.33	Poland		pl
Character Replacement	wwsi.esu.pl	212.91.7.33	Poland		pl
Character Replacement	wwsi.wdu.pl	188.128.255.251	Poland		pl
Character Insertion	wwsi.edfu.pl	89.161.146.37	Poland	edfu.pl	pl
Singular or Pluralise	edus.pl	212.91.6.58	Poland		pl
Vowel Swap	wwse.edu.pl	212.59.244.22	Poland	mail.wwse.edu.pl	pl
Vowel Swap	wwsi.adu.pl	85.128.150.243	Poland		pl
Vowel Swap	wwsi.idu.pl	176.31.45.213	France		pl
Vowel Swap	wwsi.odu.pl	82.145.47.84	United Kingdom	odu.pl	pl
Vowel Swap	wwsi.udu.pl	212.91.7.33	Poland		pl
Bit Flipping	swsi.edu.pl	185.5.96.39			pl
Bit Flipping	wwsh.edu.pl	89.161.157.246	Poland	wwsh.edu.pl	pl
Bit Flipping	wwsi.ddu.pl	80.92.84.139	Luxembourg		pl
Bit Flipping	wwsi.edt.pl	212.91.6.58	Poland		pl
Bit Flipping	wwsi.edu.pm	91.134.137.67	BULGARIA		pm
Bit Flipping	wwsi.edw.pl	77.55.113.62	Poland		pl
Bit Flipping	wwsi.eeu.pl	94.152.8.3	Poland	eeu.pl	pl
Bit Flipping	wwsi.elu.pl	188.128.255.251	Poland		pl
Bit Flipping	wwsi.etu.pl	212.91.7.33	Poland		pl
Bit Flipping	wwsi.mdu.pl	77.55.114.61	Poland		pl
Wrong TLD	edu.ch	82.195.224.111	Switzerland	all03.mx.genotec.ch	ch
Wrong TLD	edu.com	52.36.119.87	United States		com
Wrong TLD	edu.de	37.228.154.104	Germany	alt1.aspmx.l.google.com	de
Wrong TLD	edu.edu	204.13.82.92	United States		edu
Wrong TLD	edu.fr	217.70.184.38	France	fb.mail.gandi.net	fr
Wrong TLD	edu.net	98.124.199.97	United States		net
Wrong TLD	edu.org	72.52.4.119	United States	localhost	org
Wrong TLD	edu.ru	194.226.214.30	Russia	ns3.runnet.ru	ru

Rysunek 14. Lista podobnych domen

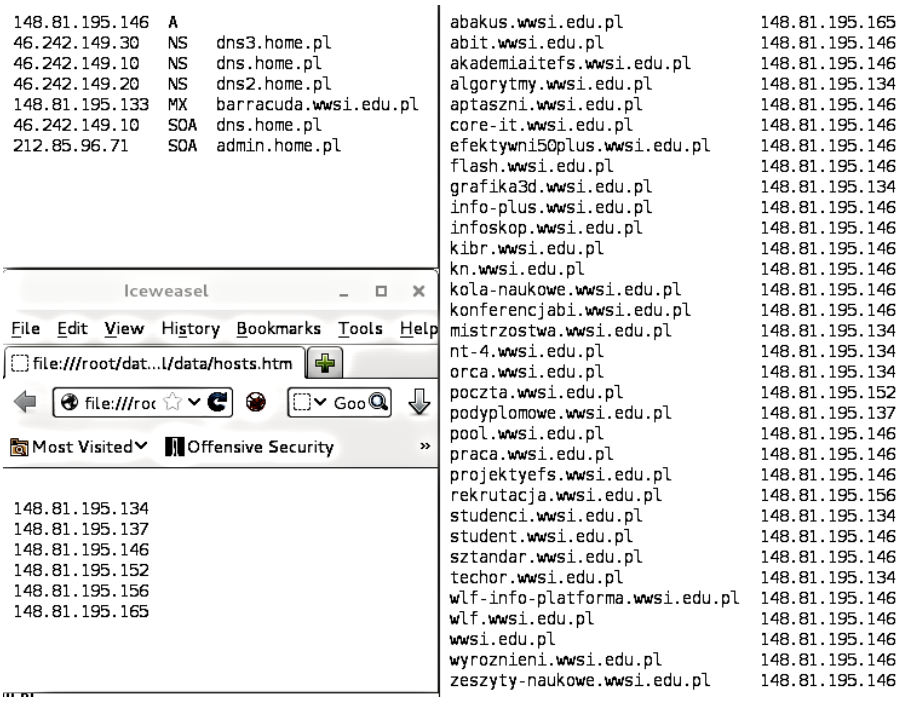
Wyciągnięta lista domen podobnych do *wwsi.edu.pl* (patrz rysunek 14), może świadczyć, że ktoś próbuje podszyć się pod oryginalną stronę w celu przeprowadzenia kampanii *phishingowej*. Jest to tak zwane zjawisko *typosquatting,* polegające na stworzeniu domeny o podobnym brzmieniu i oczekiwaniu, aż użytkownik popełni błąd w trakcie wpisywania do okna przeglądarki wybranego adresu i zostanie przekierowany do szkodliwej witryny. Mogą na niej być tylko reklamy, ale również może znajdować się złośliwe oprogramowanie, którego przykład działania został przedstawiony podczas użycia narzędzia BeFF.

```
alysakowska@wwsi.edu.pl
aptaszni@wwsi.edu.pl
azylawsk@wwsi.edu.pl
bkrzciuk@wwsi.edu.pl
bkurpiewska@wwsi.edu.pl
dmajka@wwsi.edu.pl
dziekanat@wwsi.edu.pl
ebudziak@wwsi.edu.pl
efektywni50plus@wwsi.edu.pl
informatyczna@wwsi.edu.pl
it@wwsi.edu.pl
jgolaszewska@wwsi.edu.pl
johnsmith@wwsi.edu.pl
johns@wwsi.edu.pl
john@wwsi.edu.pl
jsieruta@wwsi.edu.pl
jsmith@wwsi.edu.pl
khordejuk@wwsi.edu.pl
kstaniaszek@wwsi.edu.pl
lektorat@wwsi.edu.pl
mila@wwsi.edu.pl
mprzybysz@wwsi.edu.pl
obernadzka@wwsi.edu.pl
pbb@wwsi.edu.pl
praktyki@wwsi.edu.pl
rekrutacja@wwsi.edu.pl
rektorat@wwsi.edu.pl
rozliczenia@wwsi.edu.pl
smithj@wwsi.edu.pl
smith@wwsi.edu.pl
sztandar@wwsi.edu.pl
tduda@wwsi.edu.pl
w_wozniak@wwsi.edu.pl
```

```
NetRange:           148.81.0.0 - 148.83.255.255
CIDR:               148.81.0.0/16, 148.82.0.0/15
NetName:            RIPE-ERX-148-81-0-0
NetHandle:          NET-148-81-0-0-1
Parent:             NET148 (NET-148-0-0-0-0)
NetType:            Early Registrations, Transferred to RIPE NCC
Organization:       RIPE Network Coordination Centre (RIPE)
RegDate:            2003-10-29
Updated:            2003-10-29

ResourceLink:       whois.ripe.net

OrgName:            RIPE Network Coordination Centre
OrgId:              RIPE
Address:            P.O. Box 10096
City:               Amsterdam
StateProv:
PostalCode:         1001EB
Country:            NL
Updated:            2013-07-29

ReferralServer:     whois://whois.ripe.net

OrgAbuseHandle:     ABUSE3850-ARIN
OrgAbuseName:       Abuse Contact
OrgAbusePhone:      +31205354444
OrgAbuseEmail:      abuse@ripe.net

OrgTechHandle:      RNO29-ARIN
OrgTechName:        RIPE NCC Operations
OrgTechPhone:       +31 20 535 4444
OrgTechEmail:       hostmaster@ripe.net
```

Rysunek 15. Zestawienie zebranych danych cz. 1

Liczba uzyskanych danych jest naprawdę imponująca i po analizie materiałów osoba przeprowadzająca testy może już przygotować kilka scenariuszy ataku. Narzędzie dostarcza listę adresów e-mailowych pracowników organizacji (patrz rysunek 15) oraz wykaz adresów IP (patrz rysunek 16).

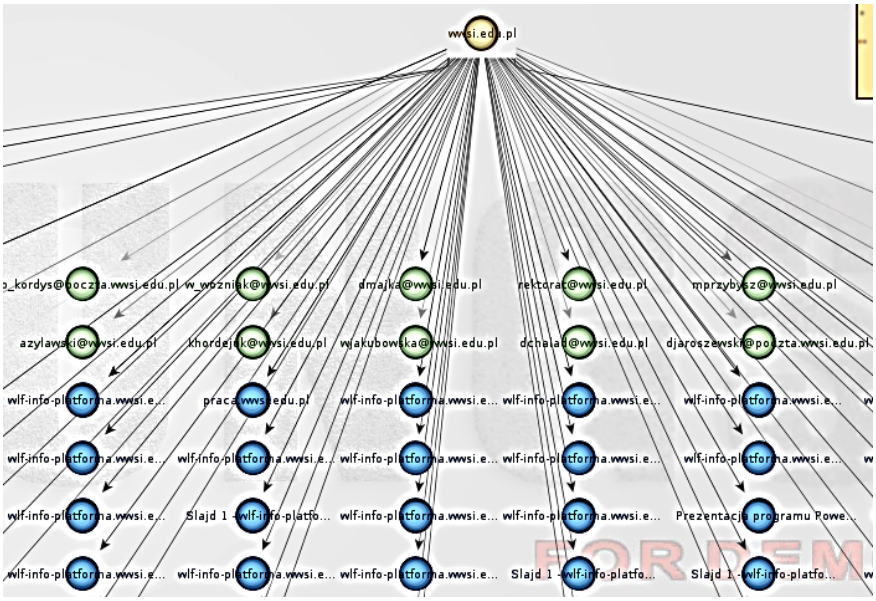


Rysunek 16. Zestawienie zebranych danych cz. 2

2.11. Maltego

Maltego [10] to bardzo dobre narzędzie do wyszukiwania i graficznego przedstawiania wyników. Zbieranie wyników za pomocą tego pakietu jest całkowicie legalne, ponieważ program ten wykorzystuje informacje ogólnie dostępne w Internecie.

Maltego poprawnie wyszukuje i obrazuje wszystkie informacje testowanej domeny. Zobrazowuje serwery domenowe z ich nazwami, serwery pocztowe, adresy IP, adresy e-mail jak również, jakie jest używane oprogramowanie (patrz rysunek 17). Narzędzie zaprezentowało wszystkie powiązane domeny i adresy poczty elektronicznej z domeną główną grupując wszystko w tabeli (patrz rysunek 18).



Rysunek 17. Wyniki działania programu Maltego

w_wozniak@wwsi.edu.pl	Email Address	w_wozniak@wwsi.edu.pl
[redacted]	Email Address	p_kordys@poczta.wwsi.edu.pl
international@wwsi.edu.p	Email Address	international@wwsi.edu.pl
email@wwsi.edu.pl	Email Address	email@wwsi.edu.pl
wski@wwsi.edu.pl	Email Address	wski@wwsi.edu.pl
mprzybysz@wwsi.edu.pl	Email Address	mprzybysz@wwsi.edu.pl
rektorat@wwsi.edu.pl	Email Address	rektorat@wwsi.edu.pl
dmajka@wwsi.edu.pl	Email Address	dmajka@wwsi.edu.pl
zgniazdowski@wwsi.edu.p	Email Address	zgniazdowski@wwsi.edu.pl
rekrutacja@wwsi.edu.pl	Email Address	rekrutacja@wwsi.edu.pl
obernadzka@wwsi.edu.pl	Email Address	obernadzka@wwsi.edu.pl
infoskop@wwsi.edu.pl	Email Address	infoskop@wwsi.edu.pl
djaroszewski@poczta.wws	Email Address	djaroszewski@poczta.wwsi.edu.pl
dchalad@wwsi.edu.pl	Email Address	dchalad@wwsi.edu.pl
wjakubowska@wwsi.edu.p	Email Address	wjakubowska@wwsi.edu.pl
khordejuk@wwsi.edu.pl	Email Address	khordejuk@wwsi.edu.pl
azylawski@wwsi.edu.pl	Email Address	azylawski@wwsi.edu.pl
wwsi.edu.pl	Domain	wwsi.edu.pl
wlf-info-platforma.wwsi.e..	Document	http://wlf-info-platforma.wwsi.edu.pl/mater...
praca.wwsi.edu.pl	Document	http://praca.wwsi.edu.pl/upload/c0/dfb760...
The Microsoft Skills Adva.	Document	http://flash.wwsi.edu.pl/wwsivideo/2013/p...
wlf-info-platforma.wwsi.e..	Document	http://wlf-info-platforma.wwsi.edu.pl/mater...
Slajd 1 - wlf-info-platfo...	Document	http://wlf-info-platforma.wwsi.edu.pl/mater...

Rysunek 18. Uporządkowana lista uzyskanych informacji

3. Podsumowanie

Przedstawione programy zostały przetestowane w stworzonym wirtualnym środowisku laboratoryjnym pod katem przydatności do używania przez osoby przeprowadzające testy bezpieczeństwa. Uzyskane wyniki potwierdziły, że programy stworzone do określonych zadań je realizują, a nawet potrafią dużo więcej. Badania zostały przeprowadzone pod kontem sprawdzenia podstawowych funkcjonalności i użyteczności narzędzi, w celu potwierdzenia ich skuteczności. Ponieważ jest ich znaczna liczba, zostały wybrane najczęściej używane.

Korzystanie z programów wymaga od osób wykonujących testy umiejętności bardzo dobrego ich obsługiwania, ponieważ tylko właściwe ustawienia mogą przynieść sukces i nie uszkodzić systemów. Jednak oprócz opisanych narzędzi bardzo ważna jest duża wiedza i doświadczenie, która pozwoli na wykorzystanie podatności jak również znalezienie pozostałych niewykrytych jeszcze błędów.

Niektóre analizowane narzędzia są dedykowane do konkretnych celów inne mają uniwersalne zastosowania, to od osoby testującej zależy i od czasu jakim dysponuje, którą opcję wybierze. Warto jednak skonfrontować pozyskane informacje używając innych programów. Analizowane oprogramowanie na każdym etapie wykonywania testów penetracyjnych potwierdziły swoją przydatność we wspomaganiu pracy pentestera. Bardzo dobrze prezentują się narzędzia, w których wyniki są prezentowane graficznie, dzięki czemu jest łatwiej przeanalizować uzyskane dane i wykonać raport podsumowujący efekty pracy.

Bibliografia

[1] https://tools.kali.org/information-gathering/theharvester
[2] https://www.whois.com/whois/
[3] https://www.netcraft.com/
[4] http://www.kloth.net/services/nslookup.php
[5] https://tools.arantius.com/dig
[6] http://it-pomoc.pl/linux/host
[7] https://tools.kali.org/information-gathering/metagoofil
[8] http://pentestit.com/foca-fingerprinting-organisation-collected-archives/
[9] http://www.thegeeky.space/2015/04/how-to-save-time-doing-passive-discovery-in-Kali-Linux-using-discover-or-backtrack-script-framework.html
[10] https://www.paterva.com/web7/docs/Maltego3TDSTransformGuideAM.pdf

Analysis of selected tools for information collection about the compromised it system

Abstract

Reconnaissance is the first step in the penetration testing process, which involves gathering information about the purpose of attack from generally available external sources. The collected data can be used to obtain, for example, employees' personal data, e-mail addresses, domain names, IP addresses of systems accessible via the Internet. In addition, information about Transmission Control Protocol (TCP) and UDP (User Datagram Protocol) services, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are available.

The reconnaissance should be done in a passive method, during which there is less risk of detecting the attacker's activity. In addition, it is a legitimate search for information available on the Internet. This method allows you to gather information without revealing that any activities are carried out. Using the selected reconnaissance programs, a lot of information about the company was analyzed.

Keywords – reconnaissance, network protocols, IP addresses, DNS systems, network services