Konrad Kurkowski

GOOGLE HACKING

Projekt realizowany w ramie przedmiotu **Przedsięwzięcie Zespołowe – Bezpieczeństwo systemów komputerowych**, pod kierownictwem dr. Adama Ziębińskiego

Dąbrowa Górnicza, 25.05.2013

1. Wprowadzenie

Roboty wyszukiwarek indeksują wszystko co napotkają na danym serwerze, który jest w danej chwili przeglądany. Istnieje zagrożenie, że wśród plików, które zostaną zindeksowane mogą się znaleźć pliki, które nie powinny nigdzie wypłynąć z danej firmy czy organizacji. Wyszukiwarka Google obecnie jest największą wyszukiwarką na rynku. Miliony stron zostało już zaindeksowanych przez wyszukiwarkę Google i codziennie zostają dodawane do wyszukiwarki nowe strony i nowe pliki. Niestety w wielu przypadkach zostają udostępnione informacje poufne, albo takie, które mogą pomóc hakerowi zaatakować nasz serwer. Można je odnaleźć za pomocą zaawansowanych narzędzi wyszukiwania. Często te narzędzia wykorzystują crackerzy, którzy za pomocą spreparowanych zapytań do wyszukiwarki Google mogą uzyskać dostęp do chronionych informacji. Dlatego ten atak dostał własną nazwę: **Google Hacking**. Bardzo często ten atak toruje drogę dla wielu innych ataków. Zaawansowane narzędzia wyszukiwania podobnie jak wcześniej wymieniona wyszukiwarka wykorzystują również niektóre inne wyszukiwarki, ale ze względu na to, iż wyszukiwarka Google jest najpopularniejsza, dlatego atak ten jest najczęściej przeprowadzany właśnie za pomocą wyszukiwarki tej firmy

2. Pojęcie Google Hacking

Google Hacking to atak polegający na wyszukiwaniu poufnych danych za pomocą wyszukiwarki google. Wyszukiwarki indeksują wszystko co napotkają na serwerze internetowym. Mogą też więc zindeksować te dane, które udostępniliśmy przypadkowo (np. listy użytkowników i haseł, listy pracowników firmy, ważne dokumenty firmowe, bazy danych itp.). Zwykle z poziomu strony internetowej te dane są nie widoczne. Wydaje się, że użytkownik nie będzie miał do nich dostępu (np. musiałby znać nazwę pliku). Jednak jeżeli w wyszukiwarkę google wpiszemy odpowiednie zapytanie możemy łatwo odnaleźć te pliki.

Dzięki Google możemy odnaleźć nie tylko informacje ogólnodostępne, lecz także miejsca, o których nie powinniśmy w ogóle wiedzieć: pliki z hasłami oraz nazwami userów, witryny zawierające luki, informacje na temat serwera, i wiele wiele więcej. Wymienione wcześniej rzeczy to jedynie garstka możliwości wyszukiwarki o której mowa. Cała sztuka wyszukiwania polega na odpowiednim zapytaniu. Otóż aby otrzymać interesujący nas wynik będziemy musieli dobrać odpowiednie operatory pytające wyszukiwarki, to właśnie w nich tkwi cała siła wyszukiwarki:

allintitle - zwraca wyniki, które zawierają wszystkie słowa kluczowe w tytule strony. operator ten nie nadaje się do łączenia z innymi elementami składni

allinurl - zwraca wyniki, które w adresie zawierają wszystkie szukane słowa, operator ten nie nadaje się do łączenia z innymi elementami składni

cache - wyświetla kopię strony lub dokumentu, którą przechowuje google. Dokument lub strona nie musi istnieć w sieci, lecz może jeszcze być zaindeksowany w google.

daterange - ogranicza wyszukiwanie od określonej daty lub przedziału czasowego, w którym strona została zaindeksowana przez wyszukiwarkę google

define - wyszukuje definicje

filetype - wyszukuje pliki o podanym rozszerzeniu

file – wyszukuje pliki o podanej nazwie

inanchor - zwraca dokumenty zawierające odnośniki, które zawierają w treści linki zawierające wyszukiwane wyrazy

info - funkcja która pokazuje nam informacje o danej stronie (jej kopię zrobioną przez google, strony podobne do niej, zawierające linki, podstrony, przeszukanie strony).

intext - zwraca wyniki zawierające wskazane słowa kluczowe w treści strony

intitle - wyświetla wyniki zawierające wskazane słowa kluczowe w tytule strony

inurl - zwraca strony, które w adresie zawierają szukane słowa

link - wyświetla linki zwrotne, które prowadzą do danej witryny

numrange - ogranicza wyszukiwanie do wyników zawierających liczby z podanego zakresu

related - wyświetla strony, które są tematycznie podobne do danej witryny

site - zawęża listę wyników do konkretnej witryny, domeny, lub grupy domen

+ (plus) - podane wyrażenie [wyraz] musi znaleźć się na stronie, nawet w przypadku ignorowania przez google takiego słowa ze względu na powszechność

- (minus) - z rezultatów wyszukiwania zostaną odjęte strony zawierające podane słowo

" " - w wynikach wyszukiwania uwzględnia całe podane frazy, nie tylko pojedyncze wyrazy zawarte w wyszukiwanych frazach

Tylda (~) – słowo, przed którym jest wstawiona, może zostać zastąpione synonimem

(kropka) – zastępuje dowolny znak

(OR) – wyszukuje strony dla zapytania: słowo lub słowo.

***** - zastępuje dowolny ciąg znaków

O czym musisz pamiętać?

1. Algorytm google ogranicza wprowadzanie do 10 słów w zapytaniu, w tym operatory logiczne (jeżeli liczba operatorów wraz z wyrazami przekroczy liczbę 10, nie będą one brane pod uwagę).

2. Możesz wykorzystywać operator * (wykorzystywanie słów zastępczych) który nie jest brany pod uwagę.

3. Posługuj się wieloma językami, dzięki temu zwiększysz pole wyszukiwania.

4. Kolejność wpisywanych słów, oraz ilość wpisywania tych samych słów ma znaczenie w wyszukiwaniu.

5. Jeżeli jakaś strona lub dokument już nie istnieje, kliknij na kopię tego dokumentu, na około 95% google umożliwi ci przejrzenie.

Stosowanie zaawansowanych metod wyszukiwania i stosowanie powyższych zasad nie od razu zrobi z nas hakerów. Aby nauczyć się jak najefektywniejszych zapytań najlepiej jest najpierw zobaczyć jak zbudowane są takie zapytania. Możemy skorzystać z gotowych baz tego typu zapytań:

- googlehacking.tk/
- www.hackersforcharity.org/ghdb/

3. Zastosowania ataku Google Hacking

Tego typu ataki możemy zastosować na wiele sposobów, które możemy ze sobą łączyć. W tym rozdziale zostaną przedstawione najczęstsze zastosowania tego ataku.

3.1 Wyszukiwanie plików

Google pozwala na odszukanie plików o danym rozszerzeniu za pomocą operatora filetype, dzięki temu możliwe staje się odszukanie interesujących nas plików, takich jak:

***.db, *.mdb** - rozszerzenia plików baz danych, mogą zawierać hasła, spis oraz dane użytkowników, itp.
***.sql** - plik zawierający kod SQL
***.inc** - plik includowany, częstym błędem a raczej niedopatrzeniem jest nieumieszczenie przez administratora pliku konfiguracyjnego serwera, który uniemożliwia patrzenie na kod pliku inc.
***.ini** - plik konfiguracyjny, zwykle zawiera ustawienia programów.
***.cfg, *.conf** - przykładowe rozszerzenia plików konfiguracyjnych różnych aplikacji.
***.bak** - plik zawierający poprzednią wersję pliku o takiej samej nazwie (kopia zapasowa), lecz innym rozszerzeniu, czyli tzw backup, może zawierać hasła, listy użytkowników, dane, itp.

***.js, *.jsp** - plik, który zawiera kod JavaScript
***.log** - plik, w którym zapisywane są logi, wydarzenia, które zostały zarejestrowane przez system operacyjny najczęściej są to: przebieg instalacji, monitorowanie ruchu na stronie, itp.
***.xls** - arkusz programu excel, może zawierać dane statystyczne, wykresy, zestawienia, dane pracowników itp.
***.txt** - plik zawierający czysty tekst z podstawowymi elementami formatowania, może zawierać kontakty telefoniczne oraz z komunikatorów, notatki, itp.
***.doc** - plik dokumentu, format charakterystyczny dla programu MS Word, przeważnie możemy z nich uzyskać CV, podania, życiorysy, informacje dot. danych osobowych.
***.vcf** - plik vcf(ang. vCard File), vCard może zawierać inf. o personaliach, kontaktach, telefonach.

Mimo iż nie jest z góry ustalone, co znajduje się w plikach z danymi rozszerzeniami, ale można podejrzewać co mogą zawierać. Musimy polegać tylko i wyłącznie na własnej twórczości, gdyż nie ma konkretnej zasady jak szukać hasła, dane osobowe, kontakty telefoniczne lub kontakty komunikatorów internetowych, które nie powinny być ogólnodostępne. Metod jest naprawdę wiele, na wyszukanie tych informacji, które w ogóle nie powinny być ujawniane.

Przykładowe zapytanie: filetype:pdf – znajdziemy wszystkie pliki o rozszerzeniu pdf

3.2 Poszukiwanie danych osobowych

Poprzez Google możemy uzyskać dokumenty jakiejś osoby, w których doszukamy się: jego imienia i nazwiska, jego adres zamieszkania, numer PESEL, telefon kontaktowy, adres email, skończone szkoły, miejsce pracy, odbyte kursy, posiadane kat. prawa jazdy, itp. Takie dane możemy uzyskać za pomocą wyszukiwania np. dokumentów Curriculum Vitae czyli, w skrócie CV szukających dobrej posady są absolwenci wyższych uczelni. Teraz musimy zastanowić się gdzie mogą znajdować się takie dokumenty. Niektóre uczelnie udostępniają swoim uczniom miejsce na serwerze, które mogą w dowolnym celu wykorzystać, choćby do przechowywania swoich dokumentów, prac, kontaktów itp. serwery te przeważnie są zaparkowane w domenach .edu i/lub .edu.pl jeśli chodzi o polskie uczelnie, choć nie koniecznie tak musi być, dlatego też nie zalecam ograniczania się tylko do domen z końcówką .edu czy też do .edu.pl.

przykłady najprostszych zapytań:
cv intitle:index.of site:edu.pl - curriculum vitae
kontakty.txt intitle:index.of - domyślny plik zaw. kontakty komunikatora GG
*.vcf intitle:index.of - pliki vCard, które mogą zawierać inf. o danych osobowych.
inurl:kontakty filetype:txt site:pl - różne kontakty
inurl:"contacts" filetype:xls - różne kontakty
inurl:"addresses" filetype:xls - różne kontakty

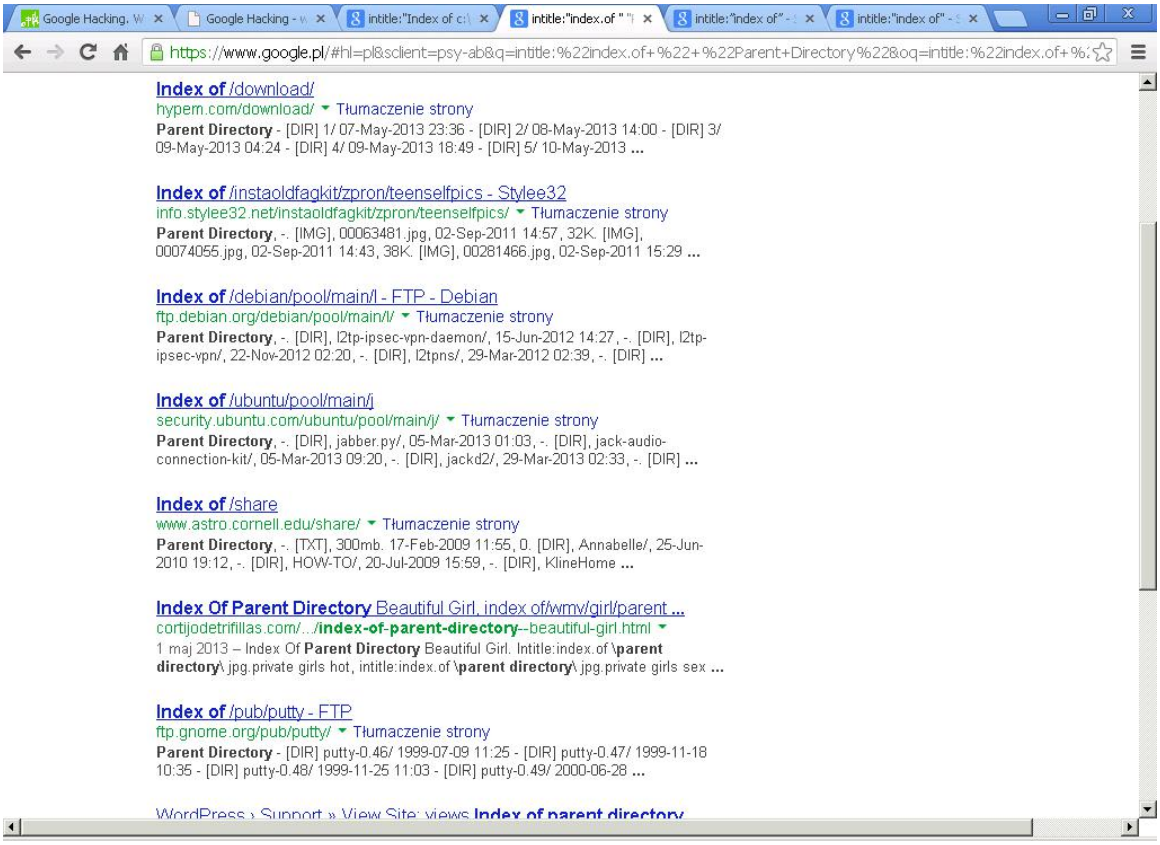
3.3 Poszukiwanie określonych serwerów lub urządzeń sieciowych

Google pozwala także na znajdowanie serwerów lub urządzeń sieciowych o określonym oprogramowaniu, oraz ich poinstalacyjne strony. Metoda polega na wklepaniu ciągu wyrazów czy znaków charakterystycznych dla danego serwera, lub dla danego urządzenia.

Dzięki wyszukiwarce google bardzo łatwo możemy uzyskać dostęp do różnych urządzeń sieciowych takich jak drukarki, routery, kamery, a także możemy zobaczyć podgląd pulpitu niektórych urządzeń oraz zobaczyć zawartość katalogów niektórych serwerów.

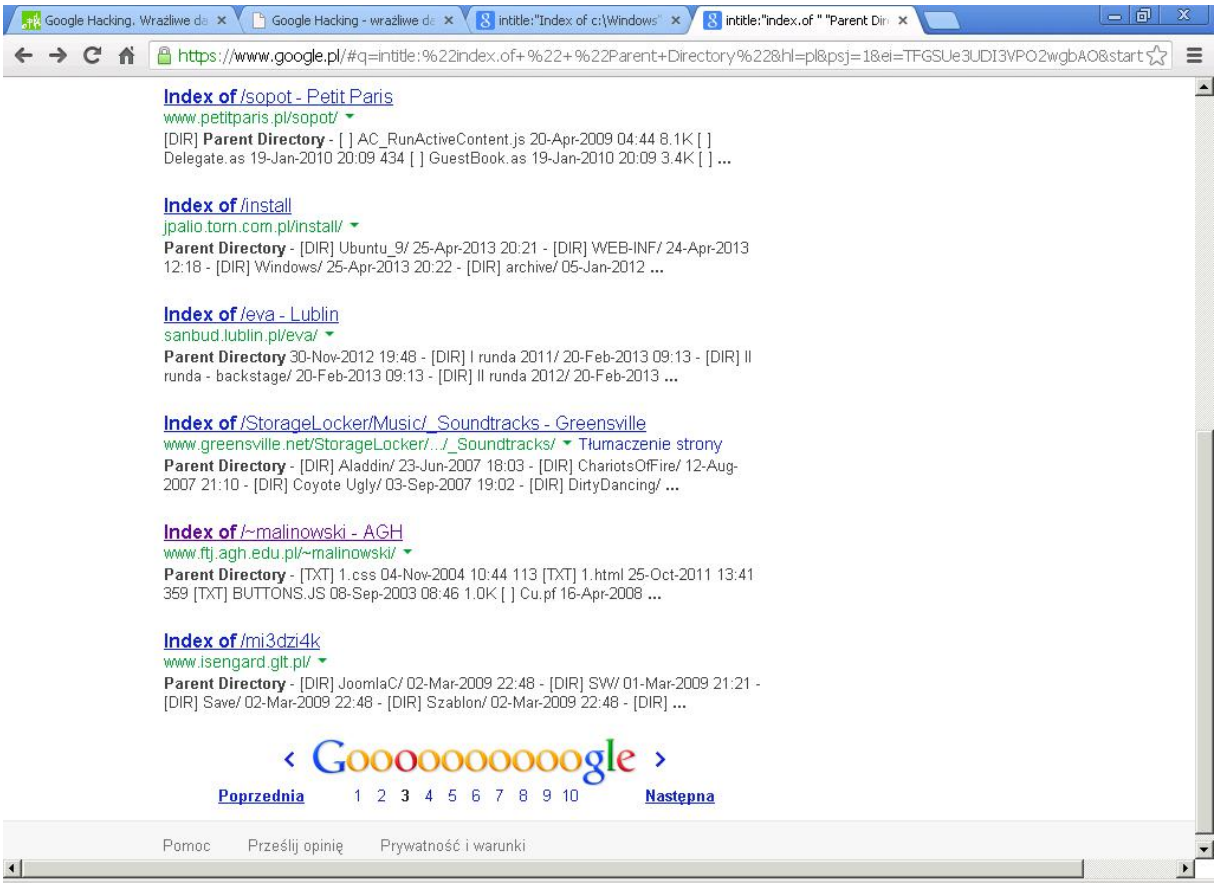
Parę przykładów:

Jeżeli wpiszemy: ***intitle:"index.of " "Parent Directory"*** – otrzymamy listę serwerów, na których można wejść do katalogów z plikami:

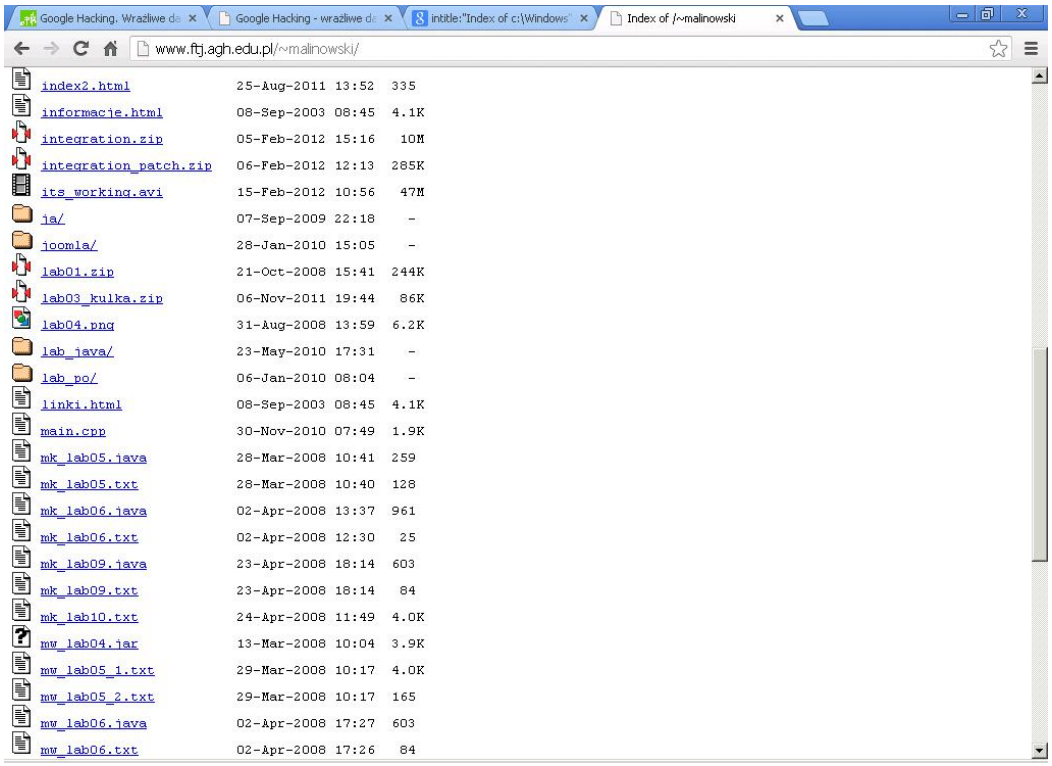


Jak widzimy są to raczej serwery ogólno dostępne. Ale jeżeli przejdziemy do strony trzeciej. To możemy znaleźć coś ciekawego:

Na trzeciej stronie może zainteresować nas taki wpis: **Index of /~malinowski – AGH**
Wygląda na to, że znajdziemy tam dane prywatne osoby o nazwisku Malinowski z AGH:

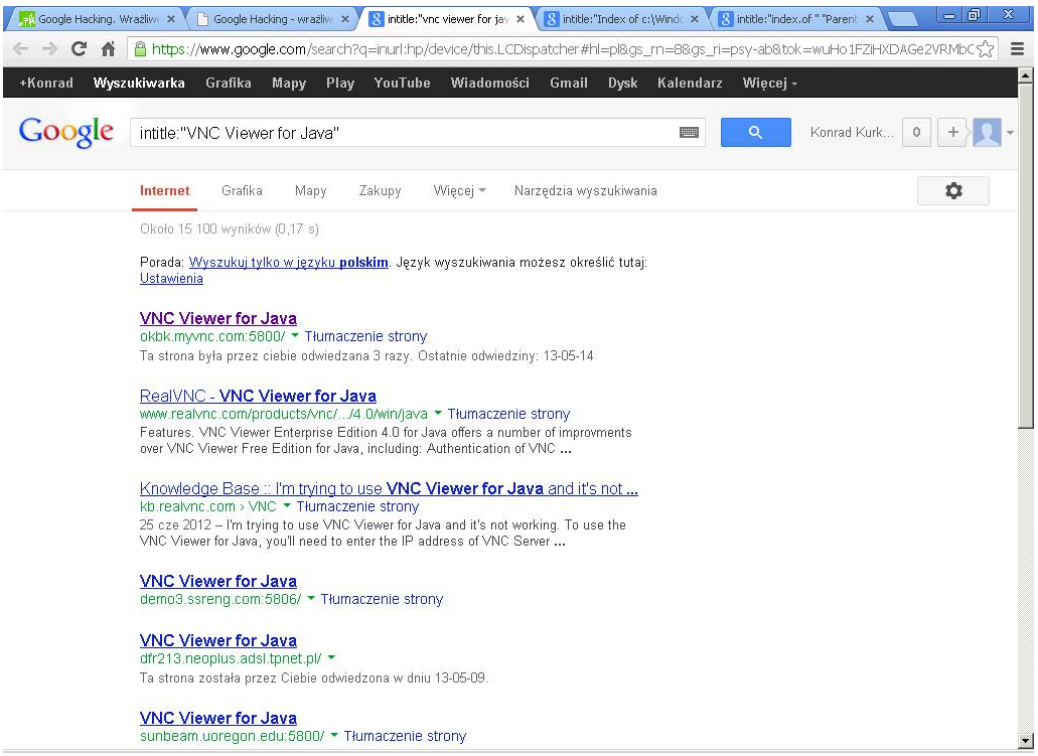


Po wejściu do tego katalogu okazuje się, że użytkownik ten posiada min. Rozwiązania ćwiczeń laboratoryjnych z jakiegoś przedmiotu. Można z dużą pewnością stwierdzić, że owa osoba nie chciała aby to się wydostało na zewnątrz.

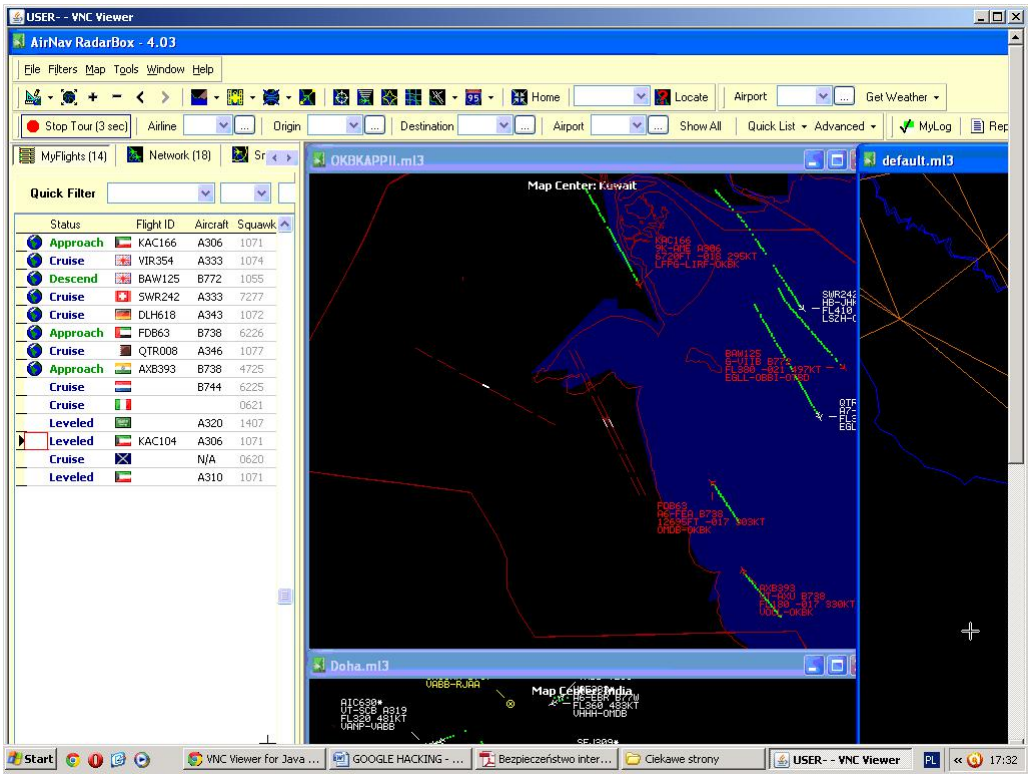


Kolejny przykład: możemy również w łatwy sposób podejrzeć czyjąś pracę na jakimś serwerze:

Wpisujemy: ***intitle:"VNC Viewer for Java"***



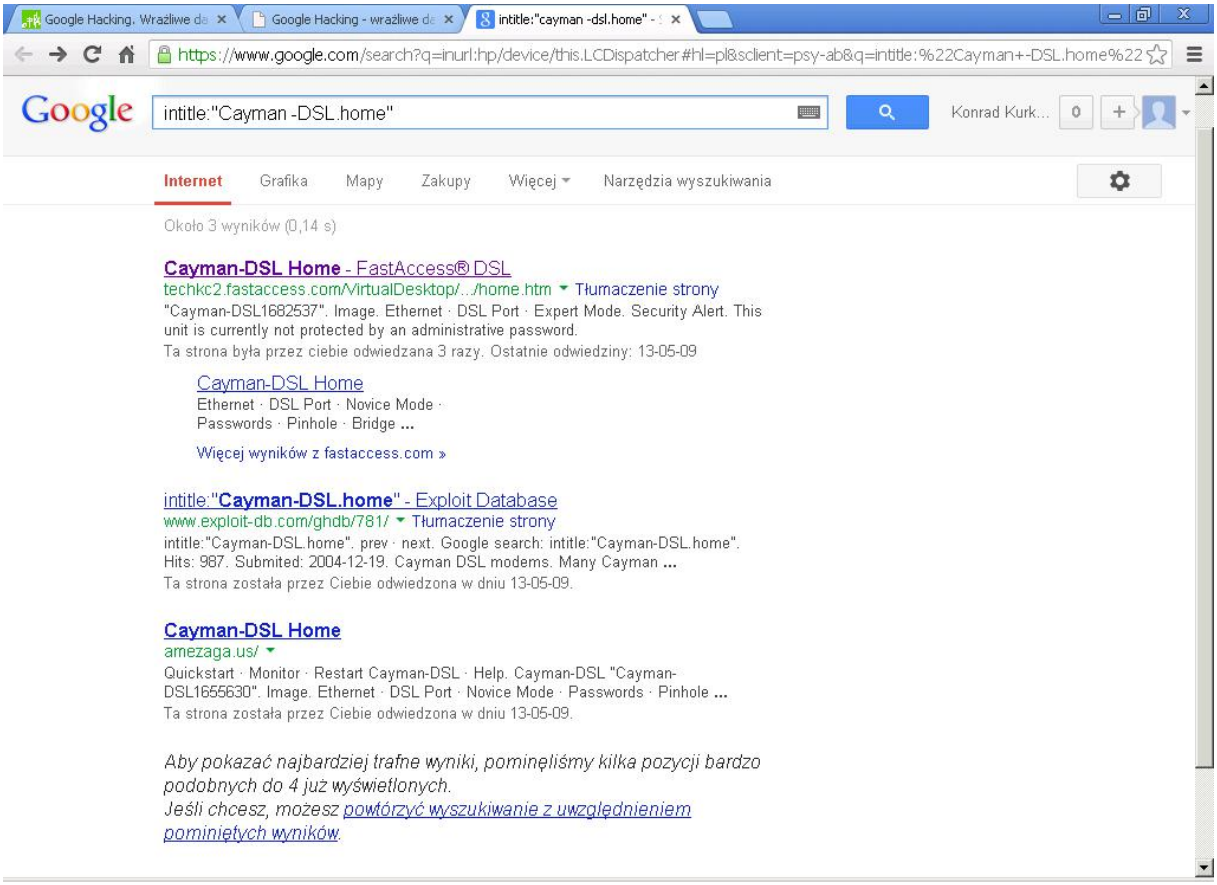
A następnie wchodzimy w pierwszy link:



Po uruchomieniu się maszyny Javy możemy się podłączyć do serwera. Ku zaskoczeniu nie jest wymagane hasło. Okazuje się, że uzyskaliśmy dostęp do podglądu z jakiegoś radaru. Dostęp do czegoś takiego moim zdaniem nie powinien być możliwy.

Kolejny przykład:

Wpisujemy: ***intitle:"Cayman -DSL.home"***



Chociaż w wyniku tego zapytania dostajemy tylko trzy pozycje to jednak na pierwszej z nich mamy coś ciekawego.

Od razu rzuca nam się w oczy informacja, że ten router, do którego właśnie się dostaliśmy nie jest zabezpieczony hasłem. Po wejściu na niego mamy więc od razu dostęp administracyjny.

Zwykle jednak jeżeli wchodzimy na jakieś urządzenie lub serwer najczęściej pojawia się prośba o hasło. Jeżeli wpiszemy jakieś zapytanie często nie od razu znajdziemy coś interesującego. Zwykle trzeba trochę po przeglądać różnych rzeczy aby coś znaleźć.

3.4 Poszukiwanie stron podatnych na błędy:

Wielu początkujących użytkowników używa gotowych, darmowych skryptów na swoje strony. Najczęściej są to fora dyskusyjne, systemy dodawania newsów, sondy, czy nawet całe systemy CMS (ang. Content Management System). Wszystkie wcześniej wymienione skrypty posiadają otwarte źródło, zatem odkrycie luki jest o wiele prostsze. Aby wyszukać takową aplikację podatną na atak, w pierwszej kolejności należy odszukać na co jest ona podatna. Zatem możemy skorzystać ze strony http://www.securityfocus.com/archive/1 , gdzie na gorąco pojawiają się luki wykryte w różnych aplikacjach, w tym również w popularnych skryptach. Potem możemy szukać wersję skryptu zawierającego błąd.

W tym celu możemy skorzystać z takich zapytań np.
"copyright by joomla" – otrzymamy listę stron opartych właśnie o ten CMS

3.5 Poszukiwanie komunikatów o błędach:

Poszukiwanie komunikatów o błędach także może przynieść potencjalnemu włamywaczowi wiele potrzebnych danych, które w późniejszym czasie wykorzysta. Błędy wyrzucane na ekran komputera mogą zawierać: nazwy plików oraz informacje dot. ich rozmieszczenia, nazwy funkcji, hasła, wersję oprogramowania, oraz wiele innych przydatnych rzeczy. Oczywiście aby odnaleźć takie strony, będzie musiał pytać wyszukiwarkę danymi frazami jakie występują w typowym błędzie, przytoczmy np. błąd autoryzacji przy połączeniu z bazą danych

Przykładowe zapytania:

"warning: mysql_connect();"
"access denied for user".

Wyszukiwarka ukaże nam wyniki, dokumenty, które wyrzucają na ekran komputera błędy.
W tym przypadku trzeba poszukać na dalszych pod stronach, gdyż często na tych pierwszych są wytłumaczenia co to jest za błąd i jak sobie z nim radzić. Jest to spowodowane tym, że strony na których faktycznie jest wyświetlony ten błąd zindeksowane są zazwyczaj na bardzo dalekich pozycjach.

3.6 Wyszukiwanie danych autoryzacyjnych:

Za pomocą wyszukiwarki Google możliwe jest również wyszukanie tzw. danych autoryzacyjnych czyli takie dane, które mogą nam pozwolić uwierzytelnić się na danym serwerze, na stronie lub w jakimś programie. Mogą to być logi, pliki konfiguracyjne i inne pliki, które mogą zawierać hasła i loginy.

Przykładowe zapytania:

filetype:log inurl:"password.log"
intitle:"index of" config.php

Tutaj nie musimy dużo szukać. Szybko natrafimy na hasło pisane czystym tekstem albo zaszyfrowane w jakiś sposób.

Przedstawione powyżej przykłady pytań to naprawdę tyko garstka sposobów na uzyskanie informacji, które nie powinny być ogólnodostępne. Takie informacje można uzyskać na kilka sposobów, wszystko zależy jednak od twórczości zapytania samego pytającego. Można przejrzeć zapytania, które są zamieszczone są w bazach tego typu zapytań (linki podałem w rozdziale drugim). Obrazują one jak wiele można znaleźć w google i jakie rzeczy udostępniają ludzie przez własną głupotę. Zapytania te możena wykorzystać również w innych wyszukiwarkach, lecz nie dadzą tak zadowalającego efektu jak google.

4. Przykładowe scenariusze ataków z pomocą google Hacking

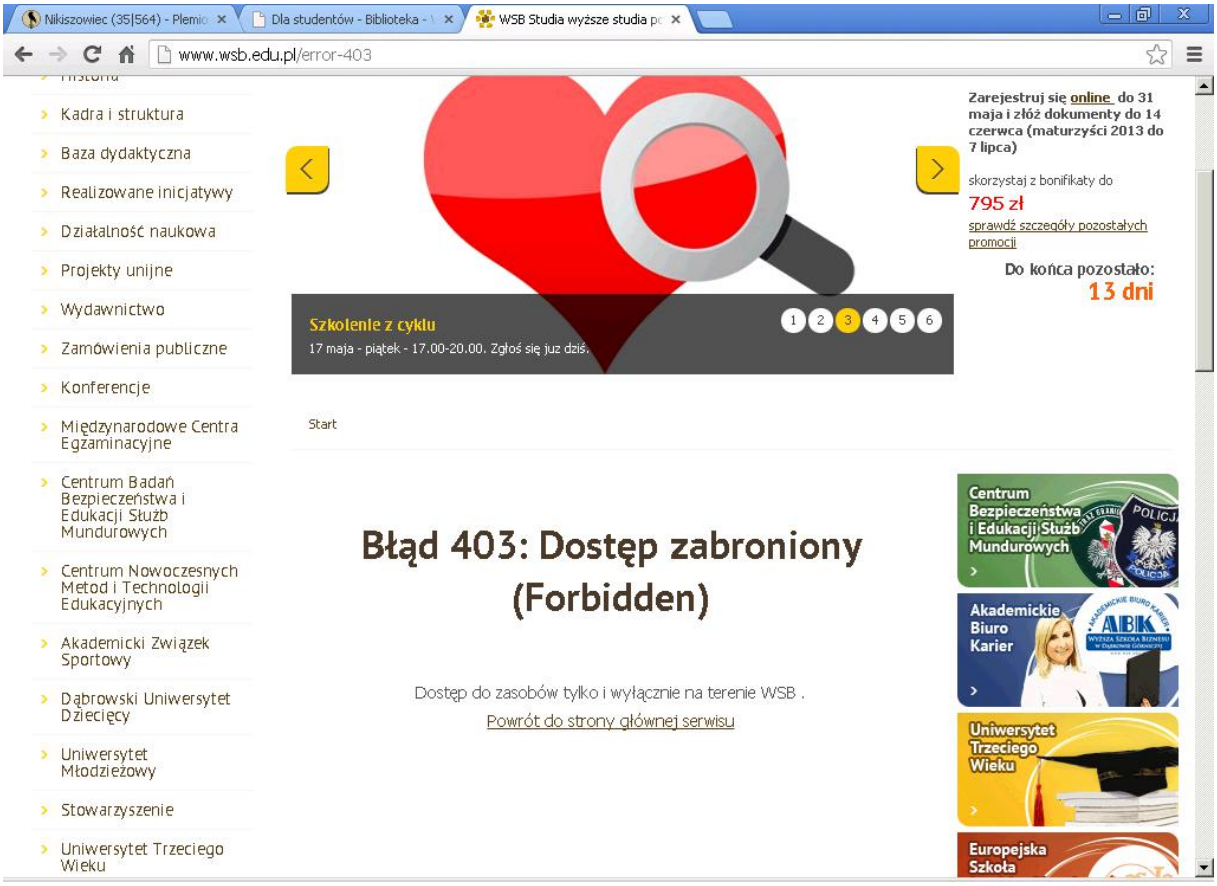
Scenariuszy ataków z pomocą Google Hacking może być naprawdę wiele. W tym artykule zostaną przedstawione trzy bardzo prawdopodobne scenariusze ataków.

4.1 Dostęp do materiałów, które można otworzyć tylko na terenie danej instytucji

Za pomocą ataku Google Hacking można uzyskać dostęp do materiałów dostępnych na terenie danej instytucji.

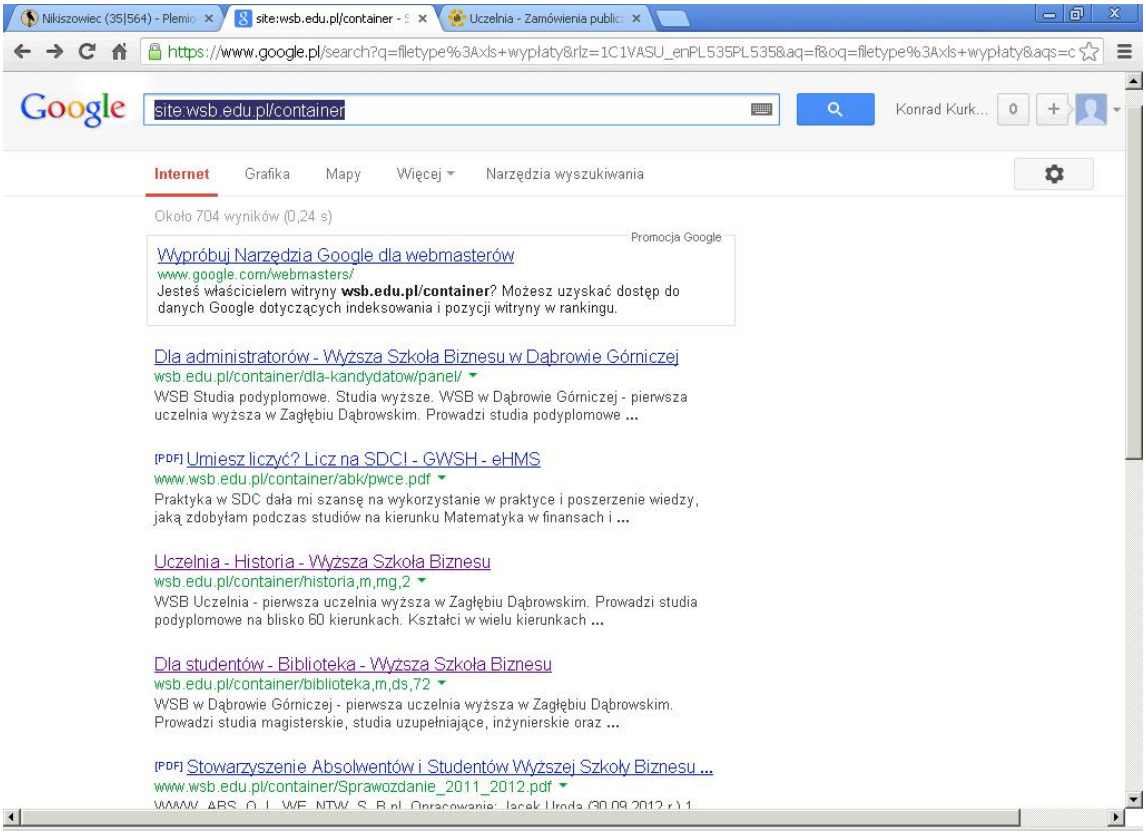
W niektórych instytucjach w ramie część strony internetowej może być dostępna tylko na terenie danej instytucji np. Wyższa Szkoła Biznesu w Dąbrowie Górniczej.

Wpisujemy w przeglądarkę adres: ***http://wsb.edu.pl/container/***



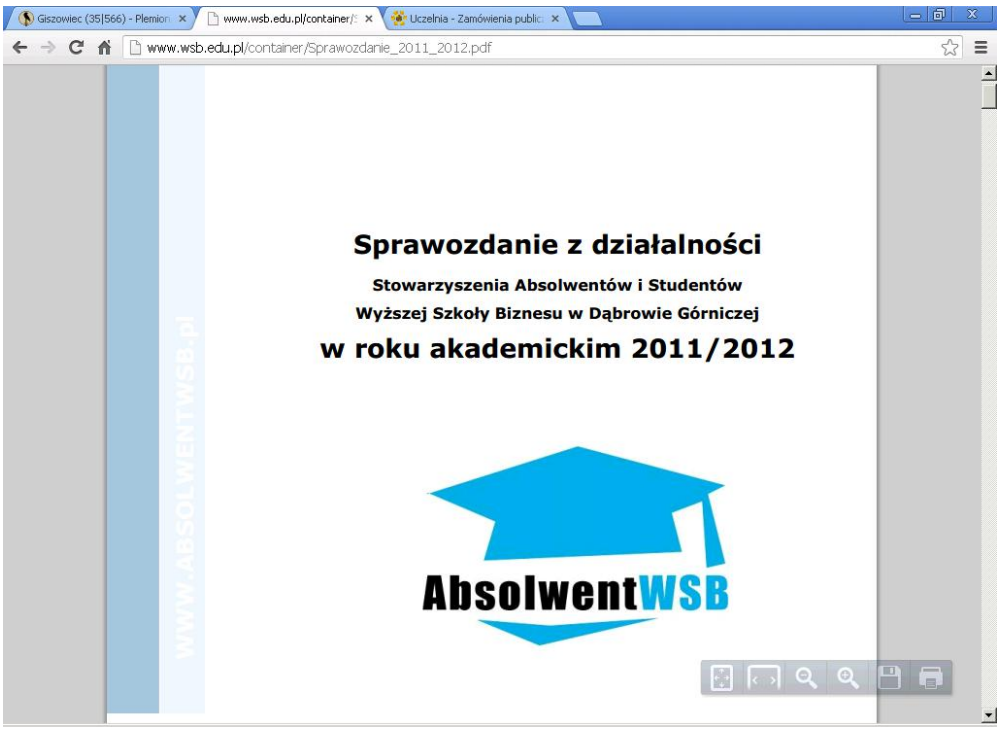
Jak widzimy dostęp do katalogu *container* z poza uczelni nie jest możliwy. Jednak za pomocą wyszukiwarki google łatwo możemy przeszukać i przejrzeć zawartość tego katalogu.

W wyszukiwarkę google Wpisujemy: ***site:wsb.edu.pl/container***



Teraz widzimy co znajduje się w katalogu *container*. Możemy teraz zobaczyć czy jest możliwy dostęp do tych zasobów.

Otwórzmy dla przykładu plik dotyczący stowarzyszenia Absolwentów i Studentów:

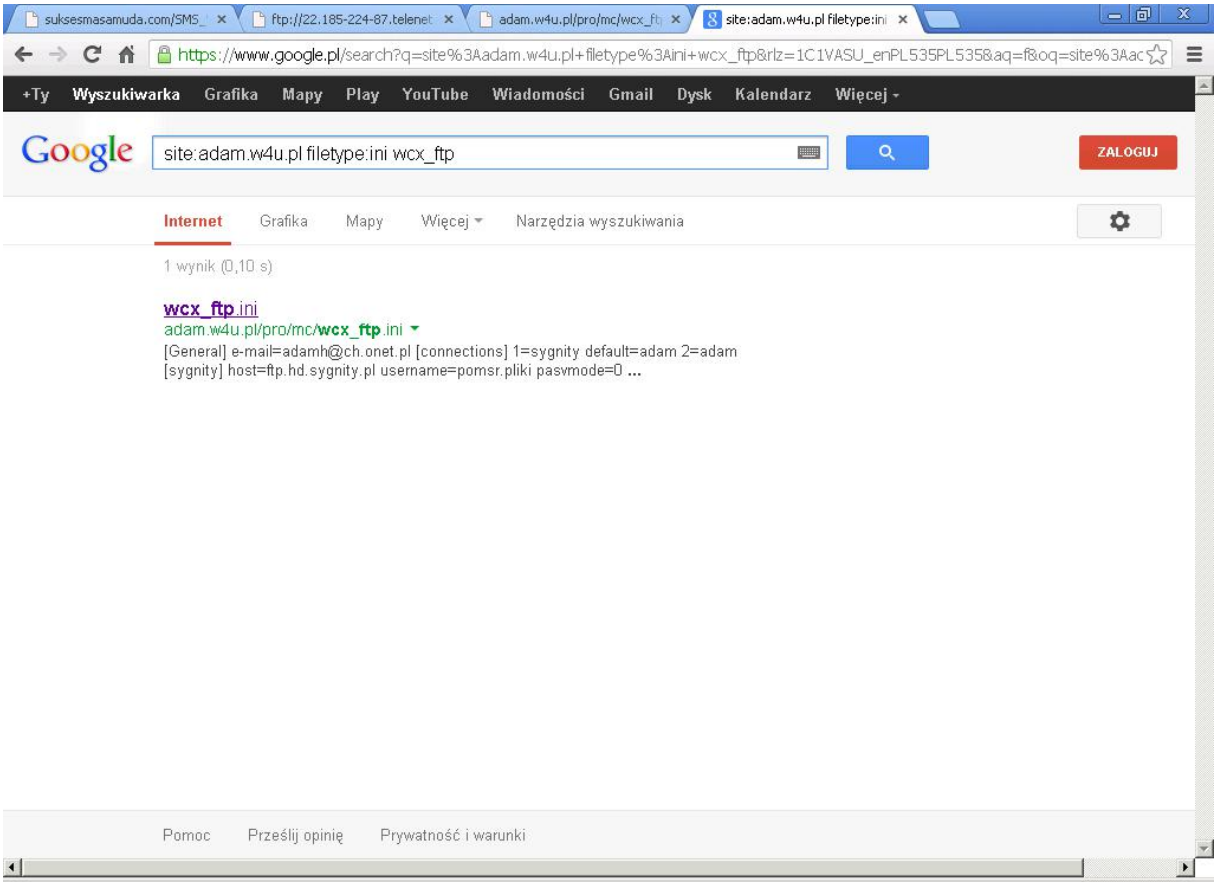


Tak więc w bardzo prosty sposób dostaliśmy się do sprawozdania z działalności stowarzyszenia.

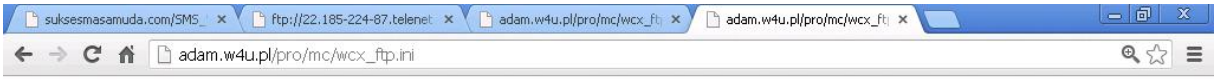
4.2 Dostęp do serwera ftp

Dzięki atakowi google Hacking możemy również uzyskać dostęp do serwera FTP. Sporo ludzi udostępnia programy na publicznie dostępnych serwerach. Jeżeli natkniemy się na pliki klienta FTP np. Total Commandera, możemy natknąć się na plik zawierający ostatnie połączenia ftp i zapisane połączenia ftp.

Ofiarą ataku niech będzie serwer adam.w4u.pl. Wiemy, że plik zawierający informacje dot. połączeń ftp nazywa się wcx_ftp.ini. Zapytanie, które wyszuka ten plik będzie wyglądać następująco: ***site:adam.w4u.pl filetype:ini wcx_ftp***



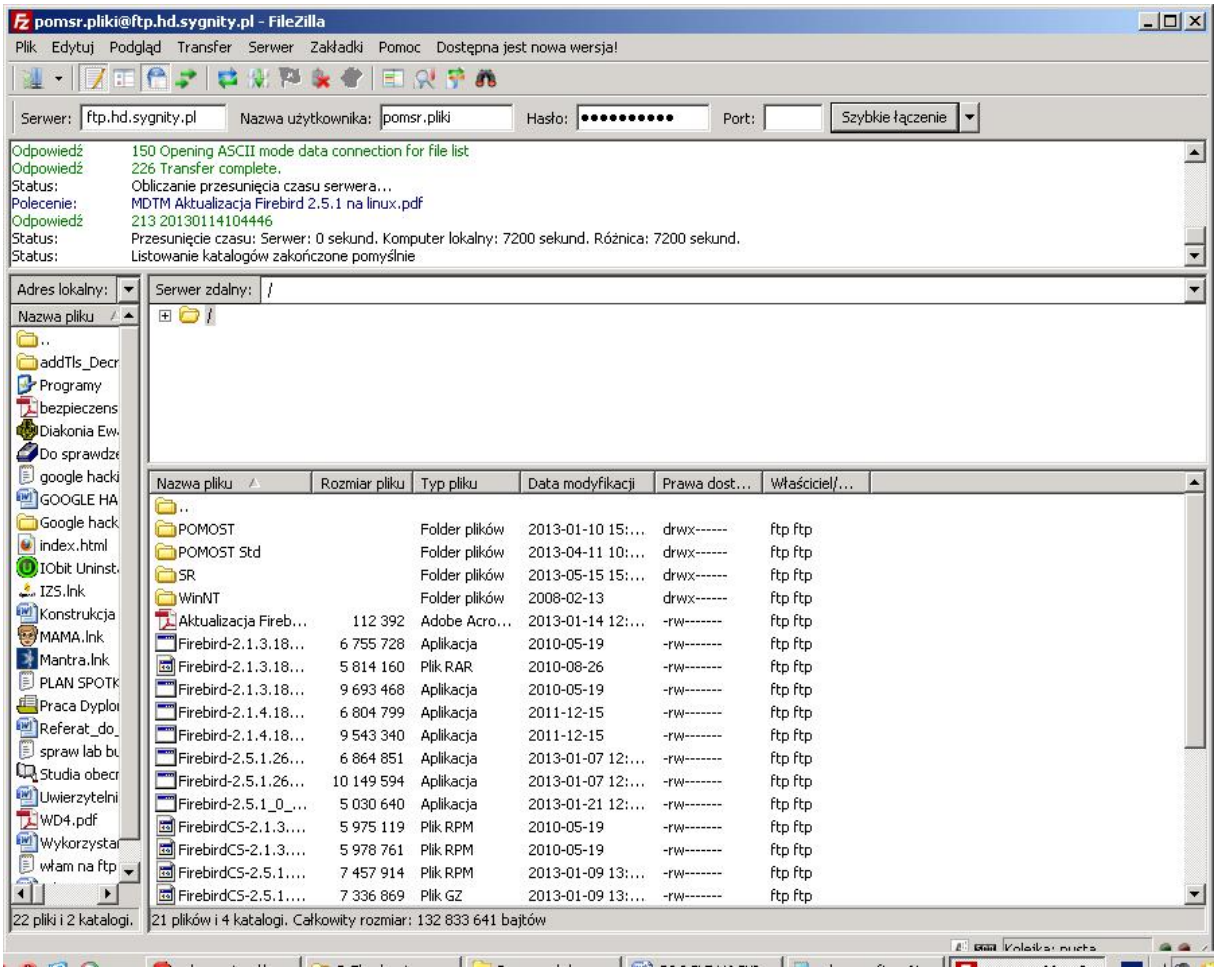
W wyniku tego otrzymaliśmy jedną interesującą nas pozycję. Możemy więc sprawdzić co ten plik zawiera:




```
[General]
e-mail=adamh@ch.onet.pl
[connections]
1=sygnity
default=adam
2=adam
[sygnity]
host=ftp.hd.sygnity.pl
username=pomsr.pliki
pasvmode=0
password=CFCBB26450E85C2ED797A9678676
[default]
pasvmode=1
[adam]
host=w4u.pl
username=adam
pasvmode=1
```

Jak widzimy mamy wszystkie dane umożliwiające nam zalogowanie się do konta, ale hasło jest w postaci zaszyfrowanej. Aby je odszyfrować wykorzystać program **Password decrypting tool for TC.** Kopiujemy zaszyfrowane hasło i klikamy **Decrypt Password.**

Hasło do tego serwera ftp brzmi więc: **#aktual125.** Mamy więc już wszystkie dane potrzebne do zalogowania na serwer. Sprawdźmy czy można się zalogować.

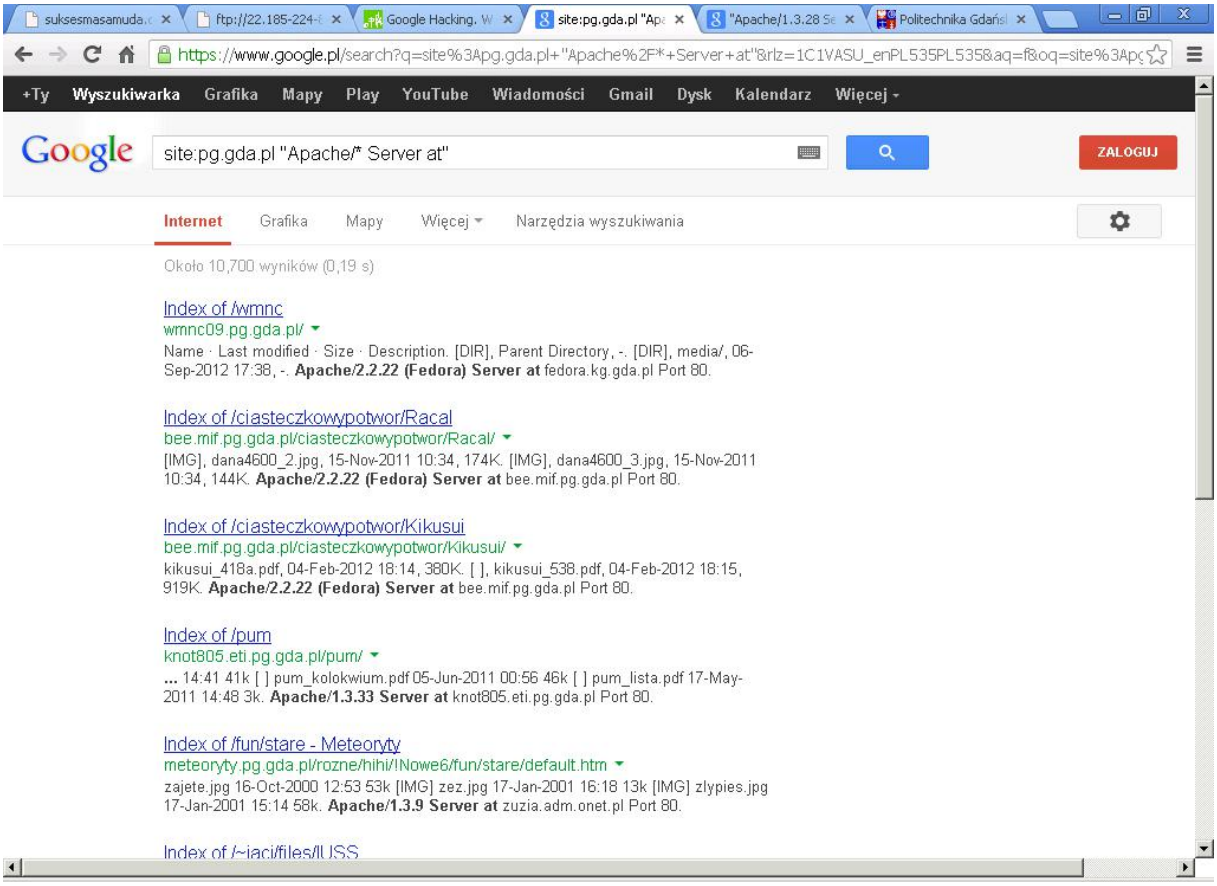


W ten bardzo łatwy sposób uzyskaliśmy dostęp do serwera ftp. Często może się zdarzyć, że natrafimy na stary plik. Wtedy nie będziemy mogli się zalogować. Zaskakujące jest jednak to, że z pomocą wyszukiwarki możemy odnaleźć dość sporo plików, które umożliwią nam dostęp do serwera ftp.

4.3 Przygotowanie do ataku na dany serwer, za pomocą wyszukiwarki google:

Możemy znaleźć wiele informacji, które mogą nam pomóc w wyszukaniu informacji na temat interesującego nas serwera, które mogą pomóc nam w przeprowadzeniu ataku. Wyobraźmy sobie, że mamy exploity dla serwera apache. Musimy wiedzieć, czy dana witryna jest obsługiwana przez serwer apache, a jeżeli tak to jaka jest wersja tego serwera.

Tym razem sprawdzimy witrynę politechniki gdańskiej **pg.gda.pl**



Zatem witryna politechniki jest postawiona na serwerze apache. Różne części strony postawione są na innej wersji serwera. Analogicznie możemy postępować, jeżeli chcemy wyszukać inne informacje dotyczące witryny, które nas interesują.

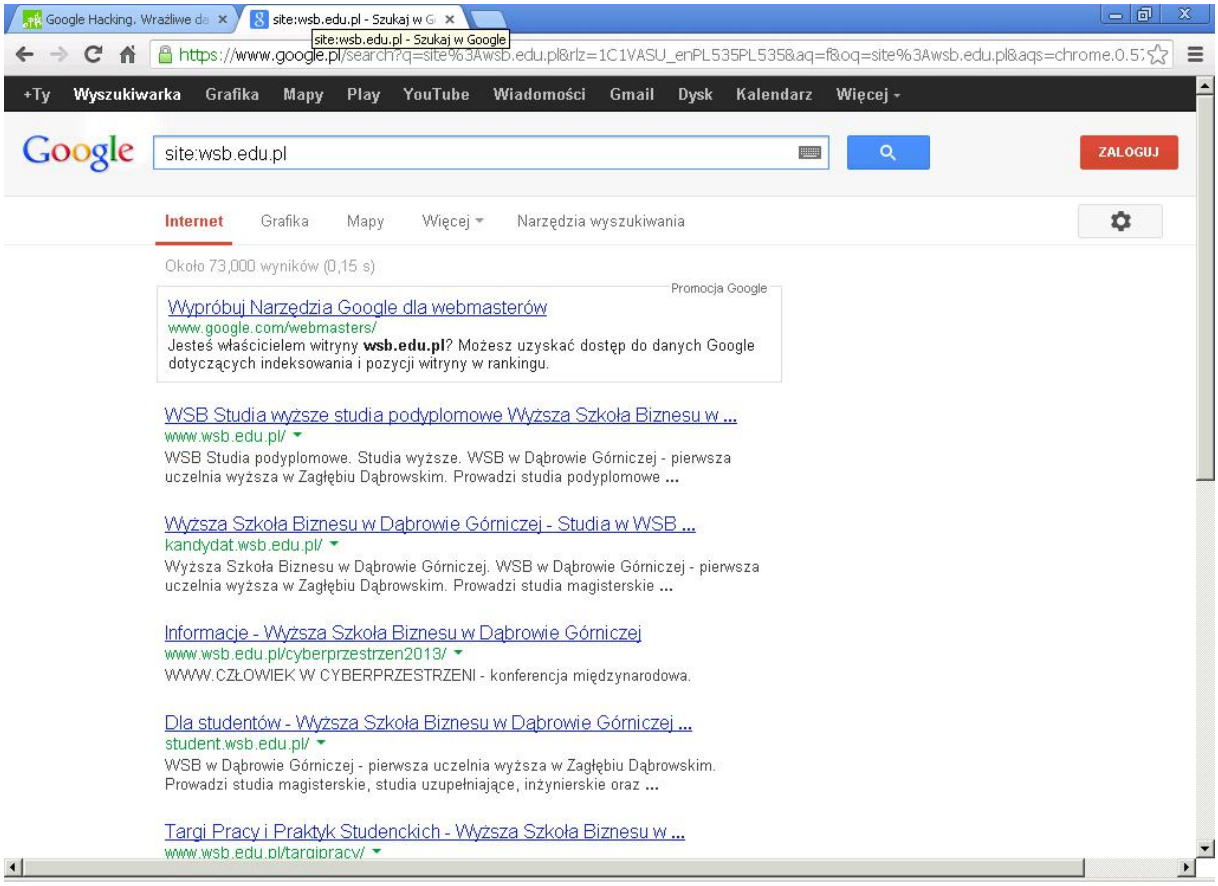
5. Metody ochrony przed atakiem

Jeśli nie chcemy narazić naszych danych na odnalezienie ich i uzyskanie dostępu za pomocą wyszukiwarki google musimy zastosować do kilku zasad, dzięki którym znacznie zmniejszymy ryzyko narażenia się na nieautoryzowany dostęp do naszych plików.

a) Należy sprawdzić, czy nie udostępniamy plików, które nie powinny być udostępnione. Powinniśmy w tym celu przeszukać katalogi, które udostępniamy.

b) Należy sprawdzić, co jest z naszego serwera zaindeksowane w wyszukiwarce:

Można to zrobić korzystając z operatora ***site***. Przy dużych witrynach może nam zająć to sporo czasu.



c) Należy skonfigurować serwer tak, aby nie pokazywał list plików:

Często możemy spotkać listę plików z danego katalogu np.

Aby się przed tym zabezpieczyć możemy zrobić kilka rzeczy:
Można ustawić chmod 700 dla folderu, dla którego chcemy, aby nie była wyświetlana lista plików

Można zastosować plik htaccess o zawartości:

Options All -Indexes

Spowoduje to, że jeżeli wejdziemy do danego katalogu, to pokaże nam się błąd 404, dlatego, że wyszukiwarka będzie szukać pliku index.html lub index.php

Innym sposobem jest też wrzucić do katalogu plik index.html lub index.php. Taki plik nie musi mieć żadnej treści.

d) Blokada dostępu dla robotów – czy plik robots.txt rozwiązuje problem?

W celu zabezpieczenia własnych danych często stosowany jest plik robots.txt w celu blokady dostępu do danych dla robotów indeksujących. Jeśli chodzi o ten plik to mamy dwie pułapki. Po pierwsze plik robots.txt nie do końca blokuje dostęp dla robotów. Jeżeli do zablokowanej treści dostępne są linki gdzieś w sieci, to google i tak to zaindeksuje. Drugą pułapką tego pliku jest to, że każdy może wyświetlić jego zawartość, a jeżeli odbierzemy mu uprawnienia, to ten plik nie będzie poprawnie funkcjonował.

Jak w takim razie zablokować możliwość dostępu do niektórych plików na serwerze. Trzeba ustawić odpowiednie uprawnienia dla wrażliwych plików i folderów. Oprócz tego z pomocą przychodzi nam plik .htaccess dzięki któremu możemy zablokować wyświetlanie danych zasobów, zastosować hasło dla katalogu, umożliwić dostęp do zasobów tylko z konkretnych adresów IP, itp.

Na temat konfiguracji .htaccess przeczytać można na **www.htaccess-guide.com**

Do blokowania dostępu dla robota google nie musimy korzystać z pliku robots.txt. Google udostępnia narzędzie „Google Webmaster Tools". Wystarczy umieścić na własnym serwerze specjalny plik, który potwierdzi, że jesteśmy właścicielem serwera. Potem mamy dostęp do wielu narzędzi. Jednym z wielu możliwości jest to, że możemy blokować całość lub część zasobów przed indeksacją.

e) Test penetracyjny

Możemy również przeprowadzić testy penetracyjne naszego serwera. Możemy to zrobić za pomocą narzędzia **gooscan**, które jest dostępne w dystrybucji linuksa o nazwie **Backtrack.**[1]

f) Ukrywanie informacji o naszym serwerze

Powinniśmy również ukryć wszelkie informacje dotyczące naszego serwera, naszej domeny, gdyż bardzo łatwo można się do nich dostać przez wyszukiwarkę. Powinniśmy ukryć bądź usunąć wszelkie informacje mówiące o tym z jakiego oprogramowania, z jakich skryptów korzystamy, ukryć informacje o tym z jakiego oprogramowania korzysta nasz serwer. Powinniśmy również wyłączyć wyświetlanie błędów na stronie. Takie informacje mogą być niezwykle cenne dla hakerów, którzy mogą chcieć nas zaatakować.

6. Podsumowanie

Potencjał ataku google Hacking jest bardzo duży. Świadomość zagrożenia jest nadal ciągle mała, a ludzi, którzy zajmują się tym atakiem choćby dla rozrywki są tysiące. Dlatego musimy kierować się zdrowym rozsądkiem przy budowaniu zawartości naszego serwera. Mam nadzieję, że niniejszy dokument przekona czytelnika jak łatwo można narazić się na atak i jak lekkomyślni bywają ludzie.

[1] Zastosowanie narzędzia gooscan, [online] 25.05.2013, http://www.securitytube.net/video/702

LITERATURA:

Konrad Kurkowski, Google Hacking – wrażliwe dane w niebezpieczeństwie, [online] 19.03.2013, http://googlehacking.tk/

Forum PC Format, Blokowanie dostępu do plików na FTP, [online]18.05.2013, http://forum.pcformat.pl/Blokowanie-dostepu-do-plikow-na-ftp-t

Krzysztof Marzec, Google Hacking, Hackin9 3/2010, s 42 – 47

Michał Piotrowski, Niebezpieczne Google – wyszukiwanie poufnych informacji, Hackin9 3/2005, s 16 – 27

Google - sztuka penetracji, [online]19.05.2013, http://www.guardians.pl/artykuly.php?art=propl_06Jul30235330.pro&cate=hacking

Maciej Laskowski, Google Hacking, [online]19.05.2013, http://knip.pol.lublin.pl/wp-content/uploads/2012/03/2e9a041-google_prezentacja.pdf