WOJCIECH SMOL

Zdalne łamanie haseł

Stopień trudności

Pokładanie nadziei w matematycznych gwarancjach bezpieczeństwa algorytmów szyfrujących i zabezpieczających dane to czysta naiwność. Każde hasło, każde zabezpieczenie można złamać... lub obejść. Niezmiennie najsłabsze ogniowo stanowi czynnik ludzki.

Z ARTYKUŁU DOWIESZ SIĘ

o atakach umożliwiających złamanie haseł do zdalnych usług,

o narzędziach służących do łamania haseł *online*,

o metodach profilowania właścicieli kont zabezpieczonych hasłem,

o metodach zbierania informacji personalnych o nieznajomych,

o zasadach tworzenia bezpiecznych haseł.

CO POWINIENEŚ WIEDZIEĆ

znać podstawy inżynierii społecznej,

orientować się w metodach przeprowadzania prostych ataków sieciowych,

znać podstawy działania i obsługi narzędzi służących do zdalnego analizowania sieci i systemów komputerowych, takich jak Nmap,

znać podstawy działania protokołu Telnet.

Istnieje wiele różnorodnych metod łamania haseł. Doboru właściwej metody należy dokonać na podstawie szczegółowej analizy konkretnego zadania. Należy rozróżnić dwa podstawowe rodzaje ataków na hasła.

Ataki typu *offline* wykorzystują fakt posiadania bezpośredniego dostępu do zaszyfrowanego pliku (np. zaszyfrowane archiwum RAR, ZIP, itd.) lub pliku zawierającego zaszyfrowane hasła (np. plik */etc/shadow* w systemach operacyjnych typu *NIX). Pomimo tego, że odzyskanie hasła bezpośrednio z postaci zaszyfrowanej, czyli odwrócenie algorytmu generującego skróty haseł, może być bardzo trudne lub praktycznie niemożliwe, posiadanie haseł w takiej postaci otwiera drogę kilku metodom ataków. Wejście w posiadanie skrótu hasła umożliwi nam wytypowanie grupy prawdopodobnych haseł, wygenerowanie dla nich skrótów zgodnie z zastosowanym w danym przypadku algorytmem, a następnie porównanie wszystkich skrótów ze skrótem łamanego hasła. W przypadku, gdy skrót hasła będzie identyczny ze skrótem któregoś ze zbioru sprawdzanych haseł, oznacza to sukces – udało nam się odnaleźć poszukiwane hasło. Większość z używanych obecnie algorytmów wyznaczania skrótu hasła jest bardzo szybka, dzięki czemu w ciągu jednej sekundy możliwe jest wygenerowanie i porównanie z wzorcem nawet setek tysięcy skrótów. Na tej zasadzie oparta została cała gama ataków – między innymi ataki słownikowe, ataki sprawdzające wszystkie możliwe kombinacje haseł (algorytmy siłowe) oraz metody hybrydowe. Najnowsze osiągnięcie w dziedzinie łamania haseł *offline* stanowią ataki oparte o tzw. tęczowe tablice. Pomysł jest dość prosty – najkrócej mówiąc, metoda ta polega na wygenerowaniu bazy zawierającej pary `<hasło, skrót hasła>` dla całego przewidywanego zbioru haseł. Specjalne metody pozwalają na zapisywanie tylko niektórych skrótów, dzięki czemu cała baza zachowuje rozsądne rozmiary. W takim przypadku odgadnięcie hasła, którego skrót posiadamy, sprowadza się do wyszukania w bazie identycznego skrótu i odczytania odpowiadającego mu hasła. Metody te są bardzo skuteczne i niezwykle szybkie, w ciągu kilku sekund możliwe jest złamanie hasła, na które tradycyjne metody sprawdzania wszystkich możliwych kombinacji potrzebowałyby dni, miesięcy, a nawet lat.

Ataki typu *offline* zostały szczegółowo przedstawione na łamach czasopisma Hakin9 (wydanie 1/2009) przez pana Łukasza Ciesielskiego. W niniejszym artykule chciałbym natomiast przedstawić ataki typu *online*. Ataki tego rodzaju można zdefiniować jako takie, w których przypadku jedyną możliwość zweryfikowania poprawności odkrytego hasła stanowi próba zdalnego zalogowania się do atakowanego systemu. Przykłady takich ataków stanowią: próba włamania się do zdalnego

serwera FTP lub próba zdobycia hasła do skrzynki e-mail dostępnej poprzez interfejs webowy.

W przypadku tego rodzaju ataków, sam proces łamania hasła ulega bardzo dużej komplikacji. Dzieje się tak, ponieważ cechą charakterystyczną sytuacji, w których używamy metod typu *online*, jest brak dostępu do atakowanego hasła w postaci zaszyfrowanej. Fakt ten uniemożliwia więc wykorzystanie ataków słownikowych, siłowych, hybrydowych oraz opartych o wygenerowaną wcześniej bazę skrótów haseł. Jak więc złamać hasło, w sytuacji, gdy nie dysponujemy żadnymi danymi na jego temat, nie posiadamy skrótu oraz nie mamy dostępu do systemu, w którym hasło to jest przechowywane? Okazuje się, że istnieją metody – zarówno techniczne, jak i pozatechniczne – których jednoczesne wykorzystanie pozwoli na złamanie takich haseł, a ich skuteczność może być zaskakująco wysoka.

Czarna magia?

Jak już wspomniałem, ataki typu *online* charakteryzuje brak dostępu do hasła w postaci zaszyfrowanej. Uniemożliwia to wykorzystanie większości klasycznych metod łamania haseł opartych o generowanie i porównywanie skrótów. Nie jest to jednak jedyny problem, przed którym stanie intruz. Ponieważ kontakt z atakowanym systemem operacyjnym lub usługą możliwy jest wyłącznie za pośrednictwem sieci (w postaci przeprowadzenia próby zalogowania), sprawdzenie pojedynczej kombinacji hasła trwa nieporównywalnie dłużej niż podobna operacja przeprowadzona lokalnie. Oznacza to więc, że w przypadku ataków *online* intruz zazwyczaj nie jest w stanie przetestować milionów czy choćby tysięcy kombinacji haseł. Ponadto tysiące prób logowania, przesyłanych do serwera poprzez publiczną sieć, może zwrócić uwagę sieciowych systemów wykrywania włamań NIDS (ang. *Network Intrusion Detection System*) i spowodować zauważenie próby włamania. Często też zdarza się, że administratorzy definiują maksymalną ilość prób logowania do danego serwera lub usługi w określonym przedziale czasu, co również uniemożliwia masowe próby zdalnego logowania.

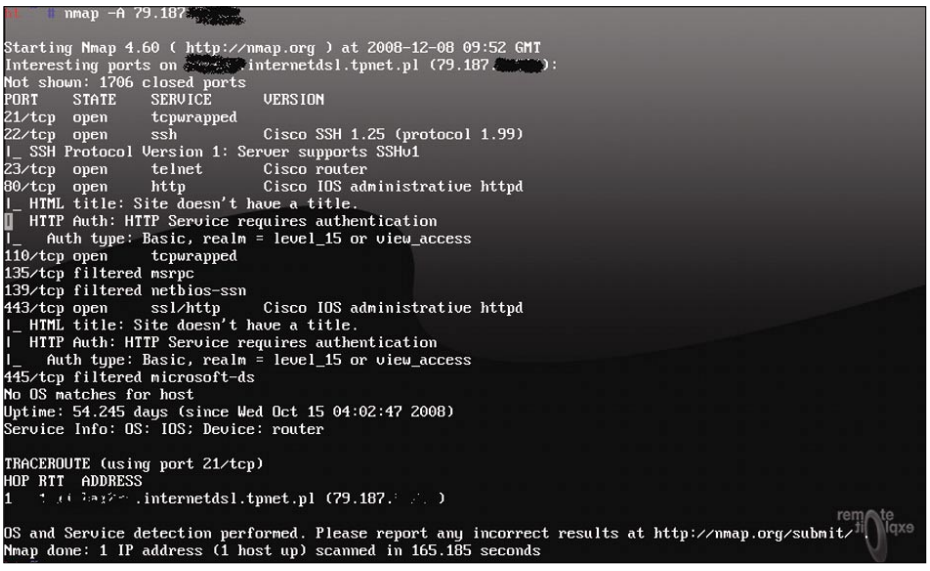
Ataki typu *online* stanowią dla intruza nie lada wyzwanie, jednak nie są niemożliwe do przeprowadzenia. Cracker może w takim przypadku wykorzystać metodę, którą można określić mianem zmodyfikowanej metody słownikowej z wykorzystaniem narzędzi automatyzujących zdalne logowanie. Cały pomysł jest dość prosty i polega na wygenerowaniu niewielkiego słownika, zawierającego tylko te hasła, co do których istnieje podejrzenie, że mogły zostać w danym przypadku użyte. Dysponując tak spreparowanym słownikiem, należy następnie skorzystać z narzędzi, które dla każdego z testowanych słów wykonają automatyczną próbę zalogowania się do atakowanego serwera lub usługi. W momencie, gdy któraś z prób logowania powiedzie się, program wyświetli prawidłowe hasło do atakowanego systemu.

Jak łatwo można się zorientować, najtrudniejszą część całej operacji stanowi wygenerowanie owego magicznego słownika potencjalnych haseł. Na pierwszy rzut oka zadanie to wydaje się praktycznie niewykonalne, bo niby na jakiej podstawie mamy tak po prostu odgadnąć czyjeś hasło? Jednak, jak za chwilę pokażę, zadanie to może się okazać zaskakująco proste. Na nic jednak zda się tutaj wiedza *stricte* informatyczna. W tym wypadku należy skorzystać z pomocy statystyki, psychologii stosowanej oraz inżynierii społecznej. Największym sprzymierzeńcem intruza może się również okazać zwykle ludzkie lenistwo oraz tak powszechne niedbalstwo...

Łamanie czarnej skrzynki

W sytuacji, gdy nie wiemy praktycznie zupełnie nic o serwerze, usłudze lub urządzeniu sieciowym (mam tu na myśli również brak wiedzy na temat osób administrujących tymi urządzeniami), do którego hasło chcielibyśmy zdobyć, mówimy o przypadku łamania czarnej skrzynki (ang. *black box cracking*). Wydaje się, że stworzenie słownika potencjalnych haseł, który posłużyłby do dalszych testów, jest w tej sytuacji niemożliwe.

Należy jednak zauważyć, że dzisiejsze serwery pracują pod kontrolą jednego z dosłownie kilku powszechnie stosowanych systemów operacyjnych. Aplikacje webowe korzystają powszechnie z kilku najpopularniejszych silników. Usługi udostępniane są za pomocą kilku najpopularniejszych rozwiązań – komercyjnych bądź darmowych. Wreszcie specjalizowane urządzenia sieciowe, takie jak przełączniki lub routery, pochodzą w głównej mierze od kilku czołowych producentów. Wniosek z tego jest taki, że intruz prawdopodobnie napotka na swej drodze dość typowe



Rysunek 1. *Nmap OS Fingerprinting*

środowisko – rzadko zdarza się, by dane rozwiązania zostało stworzone od podstaw na zamówienie. Następnie należy zauważyć, że prawdopodobnie każde z tych rozwiązań (aplikacja webowa, router, serwer bazy danych itd.) będzie udostępniało jakiś interfejs umożliwiający zdalne zarządzanie. Może to być interfejs dostępny przez przeglądarkę internetową, poprzez wiersz poleceń, protokół SNMP itd. Nie ma to jednak większego znaczenia. Najważniejsze jest to, że intruz jest w stanie taki cel zidentyfikować. Wykorzystując techniki znane jako *OS and Service Fingerprinting*, jesteśmy w stanie zebrać szereg informacji o celu ataku. Szczegółowy opis technik fingerprintingu wykracza poza temat artykułu, wspomnę tylko, że pomocny może się tu okazać znany skaner sieciowy Nmap. Gdy już zbierzemy podstawowe informacje o rodzaju systemu operacyjnego, urządzenia lub usługi, możemy przystąpić do tworzenia listy potencjalnych haseł.

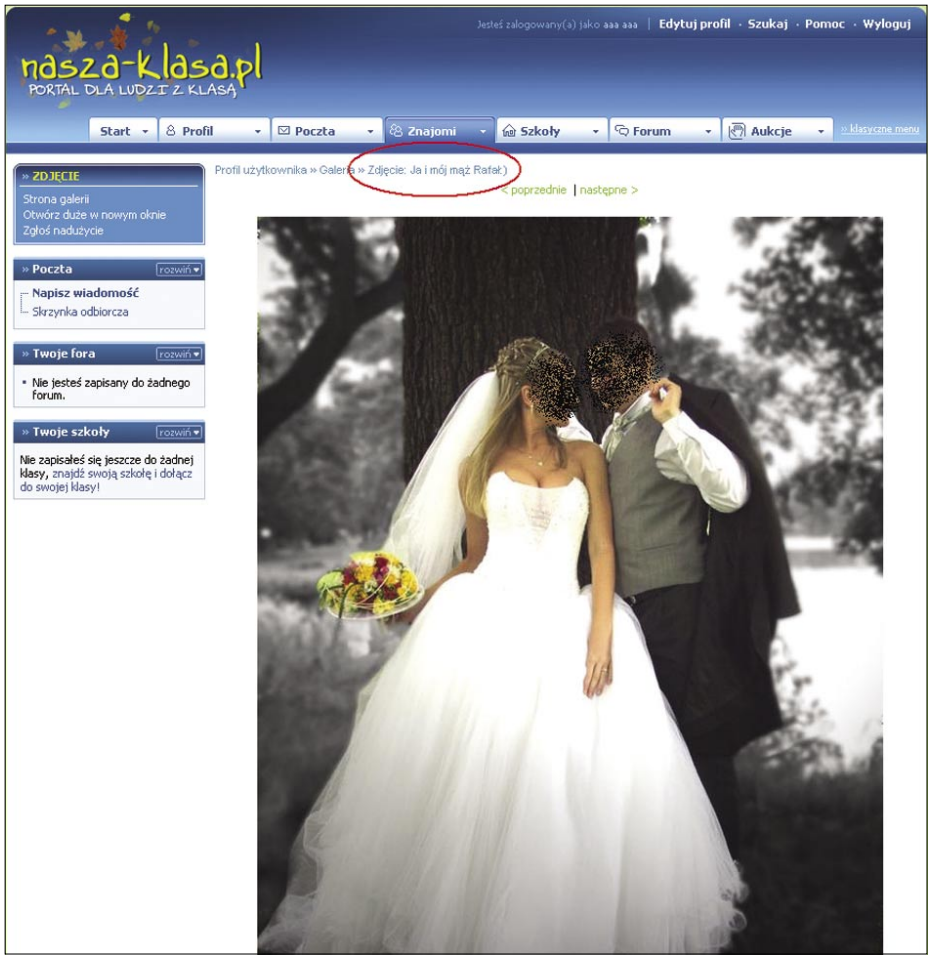
W przypadku *czarnej skrzynki* na liście potencjalnych haseł należy w pierwszej kolejności umieścić... hasła domyślnie spotykane w przypadku danego rozwiązania. Nader często zdarza się, że urządzenia lub usługi pracujące produkcyjnie nie są prawidłowo zabezpieczone. Może się więc zdarzyć, że administratorzy pozostawili domyślne konta wraz z domyślnymi hasłami i korzystają z nich produkcyjnie. Może się również zdarzyć, że administratorzy co prawda utworzyli swoje własne konta zabezpieczone silnymi hasłami i podczas pracy z nich korzystają, jednak zapomnieli wyłączyć konta domyślnie wbudowane. Zdarza się również, że na czas wdrażania i testowania nowej usługi stworzone zostało konto testowe (np. *test*) zabezpieczone łatwym do zapamiętania hasłem (np. także *test*). Spotyka się nawet takie sytuacje, w których na czas testów używa się hasła pustego! Ma to oczywiście na celu ułatwienie częstego logowania w trakcie testowania usługi – niestety zdarza się, że po uruchomieniu produkcyjnym administratorzy zapomną usunąć takie konto.

W przeciwieństwie do wielu administratorów, hakerzy oraz crackerzy znają bardzo dobrze problem haseł domyślnych lub używanych testowo i często wykorzystują tę prostą lukę. Grupy hakerskie oraz crackerskie tworzą nawet specjalne listy haseł, na których każdy może odnaleźć domyślne hasła do danego urządzenia lub programu. Jedną z największych tego typu list stworzyła i ciągle aktualizuje grupa znana jako *Phenoelit*. Korzystając z tejże listy, administratorzy mogą sprawdzić, czy przypadkiem domyślne hasła do usług i urządzeń w ich sieci nie są aktywne. Niestety, z tej bazy haseł mogą korzystać (i robią to) również crackerzy...

W drugiej kolejności należy wziąć pod uwagę wspomniane już hasła używane w trakcie testów oraz hasła najczęściej wykorzystywane. Jeśli hasła domyślne nie pozwoliły na zalogowanie się do zdalnej usługi, crackerowi pozostaje sprawdzenie haseł najczęściej wykorzystywanych. Statystyki dotyczące stosowanych haseł pokazują jasno, że ludzie wybierają zazwyczaj dość proste hasła, które są łatwe do zapamiętania oraz z czymś im się kojarzą. Listy najczęściej stosowanych haseł są oczywiście również publikowane w Internecie. Podobnie, jak w przypadku haseł domyślnych, mogą one zostać wykorzystane do sprawdzenia, czy przypadkiem stosowane przez nas hasło nie jest ujęte na jednej z list. Prawdopodobnie jednak częściej listy takie są wykorzystywane przez intruzów do stworzenia listy potencjalnych haseł. Hasła powszechnie uważane za najczęściej wykorzystywane to między innymi:

- hasło puste (brak hasła),
- słowo *hasło* lub *password*,
- słowo *admin* lub *administrator*,
- ciągi znaków występujących obok siebie na klawiaturze takie jak: *qwerty* lub *asdf*,
- hasło identyczne z nazwą konta (loginu),
- słowo niecenzuralne.

Część administratorów zdaje sobie sprawę z tego, że nie należy używać najczęściej wykorzystywanych haseł,



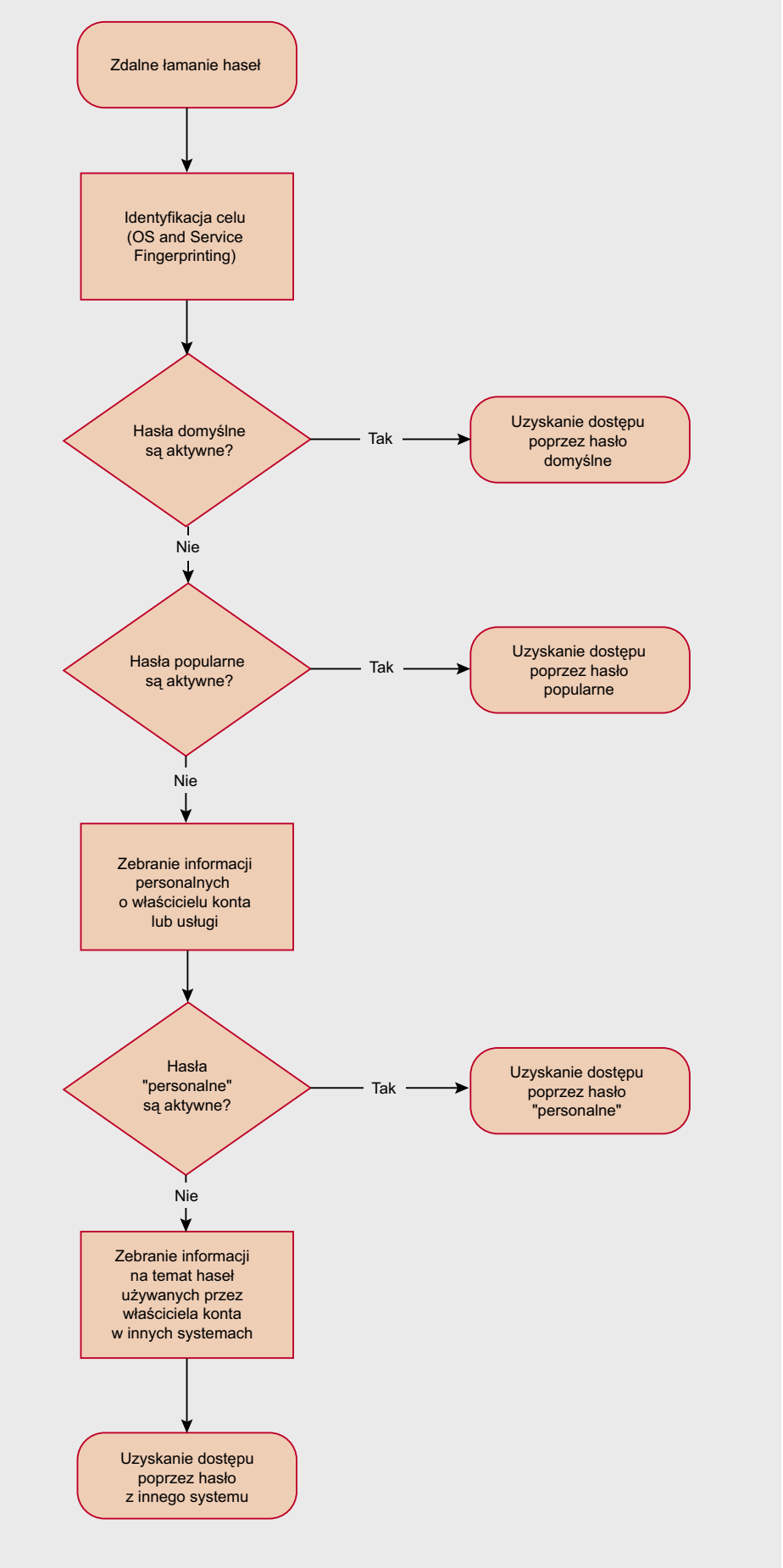
Rysunek 2. *Nieznajomych poznasz na Naszej Klasie!*

dlatego wybierają oni jedno z takich haseł... i dokonują drobnej zmiany. Chyba najczęściej stosowany dodatek do prostego hasła stanowi dodanie cyfry na końcu bądź na początku hasła. Zazwyczaj jest to po prostu cyfra 1. Wiedzą o tym oczywiście crackerzy, którzy w następnym kroku dopiszą do listy prawdopodobnych haseł kombinacje takie jak: admin1, password1, czy też 1asdf.

Jako przykład łamania hasła do systemu, o którym zupełnie nic nie wiemy, rozważmy próbę zdobycia hasła do systemu pracującego pod konkretnym adresem IP. Poza adresem IP, nie wiemy nic o celu ataku, tak więc jest to przypadek łamania czarnej skrzynki. Znając wyłącznie adres IP, atak możemy rozpocząć od próby zidentyfikowania rodzaju systemu, który pracuje pod zdalnym adresem. W tym celu wystarczy uruchomić skaner Nmap z następującymi parametrami: *nmap -A adres_IP_celu*. Przyglądając się wynikowi skanowania (Rysunek 1), można zauważyć, że Nmap zidentyfikował zdalny system jako router pracujący pod kontrolą systemu operacyjnego IOS. Przy okazji widzimy, że przeskanowany adres obsługuje łącze typu DSL w domenie *tpnet.pl*. Pod adresem IP, który wybraliśmy, kryje się więc router firmy Cisco, za którym prawdopodobnie znajduje się firmowa sieć LAN. Analizując dalej wyniki skanowania, uwagę zwracają otwarte porty urządzenia, szczególnie 23/TCP oraz 80/TCP. Otwarte dla wszystkich usługi telnet oraz zarządzania poprzez wbudowany serwer WWW świadczą o tym, że urządzenie nie zostało starannie zabezpieczone. Można więc spróbować zalogować się do urządzenia poprzez te udostępnione interfejsy korzystając z haseł domyślnych (domyślne dane umożliwiające zalogowanie się do routera Cisco to zazwyczaj: cisco:cisco) lub najczęściej używanych. Przy odrobinie szczęście uda nam się uzyskać pełen dostęp do urządzenia.

Łamanie szarej skrzynki

W przypadku braku jakichkolwiek danych na temat atakowanego systemu, przedstawione metody nie są oczywiście w 100% skuteczne, a sukces będzie



Rysunek 3. *Schemat blokowy ataku typu online*

zależał od ewentualnej słabości hasła lub zaniedbania administratora.

Jednak dość często intruz dysponuje jakąś, choćby szczątkową, wiedzą na temat atakowanej usługi lub jej administratora/właściciela. Dzieje się tak, ponieważ zazwyczaj wybrany zostaje konkretny cel ataku, a sam wybór nie jest przypadkowy.

W sytuacji, gdy dysponujemy choćby niewielką wiedzą na temat atakowanego systemu lub osób z nim związanych, mówimy o ataku polegającym na łamaniu szarej skrzynki (ang. *gray box cracking*).

Tworząc słownik potencjalnych haseł do systemu, o którym posiadamy pewną wiedzę, mimo wszystko najpierw przetestowałbym możliwości przedstawione dla przypadku czarnej skrzynki.

Jeśli hasła domyślne oraz najczęściej używane nie pozwolą na zalogowanie się do atakowanej usługi, wtedy należy wykorzystać wiedzę dotyczącą samego systemu oraz osób nim zarządzających.

Jeśli wiedza ta dotyczy samego systemu, usługi, serwera, oprogramowania lub urządzenia, do którego hasło chcemy zdobyć, tworząc słownik potencjalnych haseł można tę wiedzę wykorzystać następująco:

- wiedząc, że stworzona na zamówienie aplikacja webowa nazywa się przykładowo *GigaWebAdmin*, można spróbować poszerzyć słownik prawdopodobnych haseł o następujące loginy i hasła: *gigawebadmin:gigawebadmin*, *admin:gigawebadmin*, *administrator:gigawebadmin*, itp.; warto również przetestować hasła zawierające na końcu i na początku cyfrę, takie jak: *gigawebadmin1* oraz *1gigawebadmin*,
- jeśli system, do którego hasło chcemy zdobyć, udostępnia jakiś interfejs webowy umożliwiający rejestrację nowego użytkownika, warto się z nim zapoznać – być może będzie on źródłem cennych informacji odnośnie do wymagań oraz ograniczeń nałożonych na hasło. Dzięki temu możemy się przykładowo dowiedzieć, że hasła użytkowników systemu muszą zawierać przynajmniej jedną cyfrę; dysponując taką wiedzą, słownik prawdopodobnych haseł modyfikujemy, tak by wszystkie wpisy zawierały na początku lub na końcu cyfrę (najprawdopodobniej właśnie w ten sposób użytkownicy spełniają wymagania systemu),
- jeśli dysponujemy wiedzą na temat firmy wdrażającej dany system, również może to być dla nas cenną pomocą. Jeżeli firma ta nazywa się przykładowo *Giga Web Soft*, intruz może spróbować poszerzyć słownik o następujące loginy i hasła: *gigawebsoft:gigawebsoft*, *gigawebsoft:gigawebsoft1*, *gws:gws*, *gws:gws1*, itp.; jest wielce prawdopodobne, że na czas wdrożenia wdrożeniowcy utworzyli dla siebie konto administracyjne zabezpieczone łatwym do zapamiętania hasłem, natomiast administratorzy mogą zapomnieć o wyłączaniu lub usunięciu takiego konta.

Jeśli posiadamy jakąś wiedzę na temat osoby, której hasło do danej usługi chcemy złamać, sprawa wygląda jeszcze bardziej interesująco. W takiej sytuacji, tworząc słownik potencjalnych haseł można spróbować wykorzystać dodatkowo następujące fakty:

- znając dane personalne właściciela konta, do listy prawdopodobnych haseł można dopisać ciągi znaków związane z imieniem, nazwiskiem czy też datą urodzenia tej osoby,
- dysponując wiedzą na temat osób bliskich właścicielowi konta, warto sprawdzić hasła związane z danymi personalnymi małżonka, sympatii itp.,
- niektórzy użytkownicy, wiedząc, że dane personalne bliskich mogą być zbyt łatwe do odgadnięcia, jako hasło wybierają ciągi znaków związane z faktami, o których wie mniej osób, czyli np. imiona zwierząt domowych, nazwę ulubionego miejsca czy też imię pierwszej miłości z czasów szkoły podstawowej.

Oczywiście również te kombinacje warto testować w wersji z pojedynczą cyfrą na początku i na końcu ciągu, gdyż niezmiennie stanowi to najczęstszy sposób *urozmaicania* haseł.

Często jest jednak tak, że intruz nie zna dobrze osoby, do której konta chce się włamać. Wszak możemy dysponować imieniem i nazwiskiem administratora danego systemu komputerowego, serwera lub urządzenia sieciowego (czasem informację taką można znaleźć najzwyczajniej na stronie domowej danej firmy!), lecz poza tym nie znać żadnych danych personalnych ani dotyczących życia osobistego tejże osoby. Istnieją jednak metody pozwalające na bardzo dobre poznanie nieznajomych ludzi...

Dobry (nie)znajomy

Załóżmy, że udało się ustalić tylko imię i nazwisko właściciela konta, do którego hasło chcemy złamać. W jaki sposób możemy utworzyć słownik potencjalnych haseł, zawierający oprócz haseł domyślnych i najczęściej używanych, również ciągi związane z danymi personalnymi tej osoby oraz jej znajomych? Wystarczy skorzystać z serwisów społecznościowych (ang. *social network services*), takich jak *nasza-klasa.pl*. Portale tego typu umożliwiają użytkownikom nawiązywanie ciekawych kontaktów, poznawanie nowych ludzi oraz odnawianie starych znajomości. Niestety, aby inni mogli nas odnaleźć, zazwyczaj jesteśmy zmuszeni udostępnić o sobie szereg informacji. Znając tylko imię i nazwisko właściciela atakowanego konta oraz zakładając, że korzysta on z portali społecznościowych, możemy

```
bt ~ # hydra 83.17.[illegible] telnet -s 23 -v -l cisco -p /slownik.txt -e ns -t 36
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 3.
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2008-12-10 10:16:30
[DATA] 3 tasks, 1 servers, 3 login tries (l:1/p:3), ~1 tries per task
[DATA] attacking service telnet on port 23
[VERBOSE] Resolving addresses ... done
[STATUS] attack finished for 83.17.[illegible] (waiting for childs to finish)
[23][telnet] host: 83.17.[illegible]   login: cisco   password: cisco
Hydra (http://www.thc.org) finished at 2008-12-10 10:16:37
bt ~ #
```

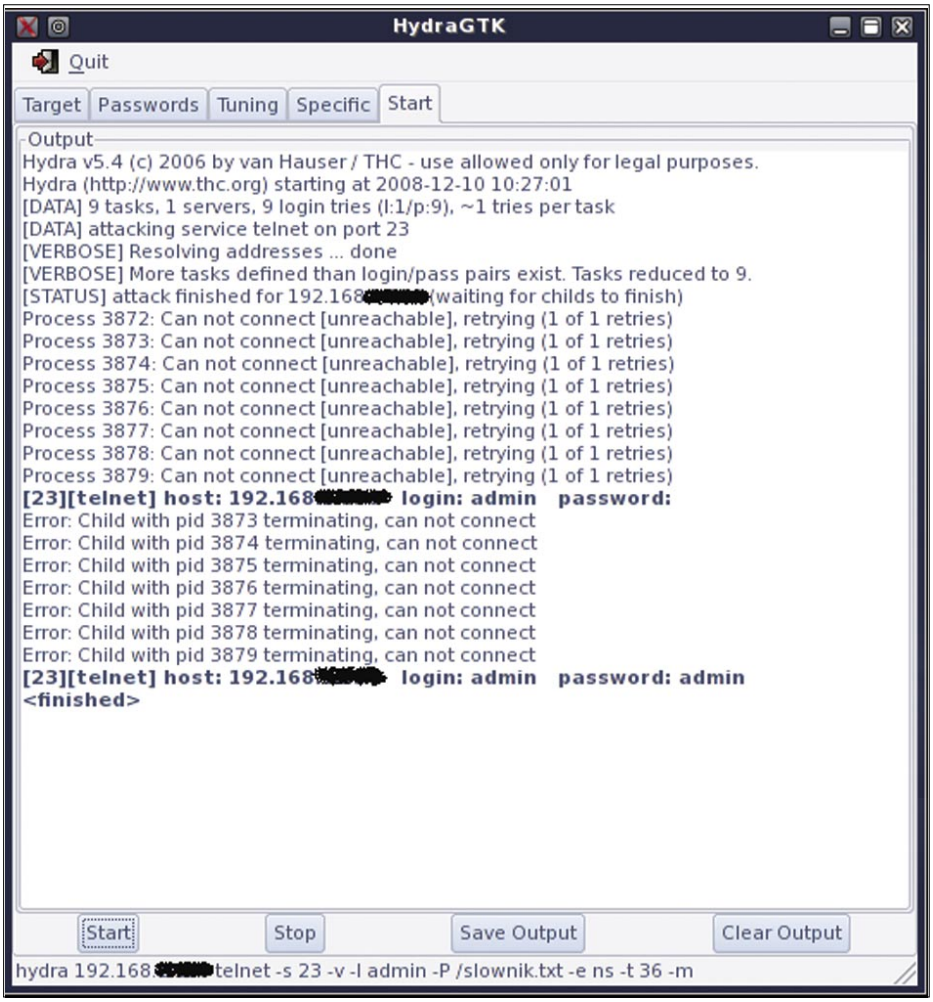
Rysunek 4. *Hydra w akcji*

zebrać szereg potencjalnych haseł. Po pierwsze, jeśli wyszukiwanie zwróci wielu użytkowników o szukanym imieniu i nazwisku, należy ustalić, o który profil dokładnie chodzi. Pomóc w tym może miejsce zamieszkania (w pobliżu firmy, w której ta osoba pracuje) oraz opis w polu *Czym się aktualnie zajmuję*. Gdy zidentyfikujemy już konkretne konto w serwisie społecznościowym, możemy zebrać szereg potencjalnych haseł na podstawie analizy profilu oraz znajomości nawiązanych z innymi użytkownikami. Przykładowe potencjalne hasła ustalone w ten sposób mogą być następujące:

- pseudonim szkolny,
- nazwisko panieńskie (zdarza się, że zamężne kobiety wykorzystują nazwisko panieńskie jako hasło, uważając, że niewiele osób z ich obecnego środowiska może je znać),
- numer telefonu,
- imię ulubionego zwierzaka domowego (w przypadku, gdy ktoś ma ulubionego zwierzaka domowego, być może w galerii dołączonej do profilu umieścił zdjęcie pupila opatrzone stosownym podpisem),
- nazwa ulubionego miejsca (przeglądamy galerię zdjęć w poszukiwaniu fotografii opatrzonych wymownym komentarzem),
- dane personalne najlepszego przyjaciela lub sympatii z czasów dzieciństwa (przeglądamy galerię w poszukiwaniu sentymentalnych zdjęć, opatrzonych komentarzem dotyczącym wspomnień),
- numer rejestracyjny (ewentualnie również marka/model) samochodu, motoru itp. (zdarza się, że w galerii użytkownicy umieszczają zdjęcia pojazdów, które posiadają),
- dane personalne bliskich (współmałżonka, rodzeństwa, dzieci) oraz przyjaciół.

W celu ustalenia, które z kontaktów danej osoby należą do jej bliskich, wystarczy zazwyczaj przeanalizować galerię zdjęć wraz z ich opisami oraz komentarze dodawane do profilu i zdjęć przez innych użytkowników portalu. Gdy już ustalimy grono osób bliskich, do listy prawdopodobnych haseł można dodać wszystkie powyższe kategorie danych, ustalone odpowiednio dla każdej z osób. Jak zwykle, dobrym pomysłem będzie dodanie kombinacji zawierających na końcu oraz na początku cyfrę, można również zawrzeć wszystkie kombinacje pisane wspak. Wszystko zależy oczywiście od tego, jak bardzo musimy ograniczyć (np. ze względu na nałożone na dany system ograniczenia liczby logowań w określonym okresie) nasz słownik haseł prawdopodobnych.

W przypadku, gdy dysponujemy innymi danymi dotyczącymi właściciela konta, można również zastosować inne techniki pozyskiwania informacji na temat prawdopodobnych haseł. Jeśli przykładowo znamy prywatny adres e-mail właściciela atakowanego konta, który został założony na publicznym serwerze, możemy spróbować wykorzystać ten fakt. Wystarczy skorzystać z formularza służącego do odzyskiwania zapomnianego hasła do skrzynki e-mail. W przypadku, gdy pytanie pozwalające na przypomnienie hasła jest dość proste (np. imię mojego psa, imię mojej pierwszej miłości), być może uda nam się odzyskać hasło do skrzynki, gdyż odpowiedzi na tego typu pytania prawdopodobnie uda się odnaleźć na wspominanym wcześniej portalu społecznościowym. Przy odrobinie szczęścia hasło do atakowanego konta będzie identyczne lub bardzo podobne do odzyskanego hasła do poczty elektronicznej. Nie jest przecież tajemnicą, że wiele osób używa zawsze tych samych (lub bardzo podobnych) haseł. Jeśli nawet hasło do docelowego konta będzie inne, da nam to przynajmniej obraz typu haseł stosowanych przez tę osobę. Jeśli uda nam się w jakiś sposób uzyskać dostęp (np. zdalnie) do komputera, z którego korzysta interesująca nas osoba, uzyskanie informacji na temat stosowanych przez nią haseł jest jeszcze prostsze. Wystarczy, że intruz złamie hasło do konta tej osoby



Rysunek 5. *HydraGTK*

w systemie Windows za pomocą przeznaczonej do tego dystrybucji Linuksa – Ophcrack. Można również w łatwy sposób odkryć hasła stosowane w komunikatorze Gadu-Gadu. Wystarczy dostęp do pliku konfiguracyjnego oraz skorzystanie z powszechnie dostępnego oprogramowania *GG Tools*. Wszystko to oczywiście również umożliwi intruzowi bardziej precyzyjne określenie potencjalnych haseł przy ataku na docelowe konto użytkownika.

Idąc dalej, w celu poznania przykładowych haseł stosowanych przez analizowaną osobę, intruz może się posłużyć również zaawansowanymi metodami socjotechnicznymi. Przykładowo, ustalając zainteresowania atakowanego (ponownie pomocny okaże się portal społecznościowy), można jej przesłać mailem zachętę do utworzenia własnego profilu w specjalnie spreparowanym forum tematycznym. Dzięki temu również możemy dowiedzieć się, jakiego typu hasła osoba ta stosuje.

Jak widać, pomysłowy intruz dysponuje całą gamą możliwości ustalenia listy prawdopodobnych haseł używanych przez ofiarę. Jako podsumowanie proponowanej przeze mnie procedury ataku typu *online* utworzyłem schemat blokowy, według którego intruz może taki atak przeprowadzić (Rysunek 3).

Przedstawione przykłady to zaledwie kilka pomysłów, możliwości w tym zakresie są niemal nieograniczone. Po żmudnym procesie tworzenia takiego słownika pozostaje już tylko przetestowanie jego skuteczności.

Wścibska Hydra

Dysponując stworzonym uprzednio słownikiem potencjalnych haseł do systemu lub usługi, którą chcemy złamać, nie pozostaje już nic innego, jak wykonanie właściwego ataku. W przypadku ataków typu online przygotowany słownik może zawierać od kilkunastu do kilku tysięcy haseł. Tworzenie obszerniejszych słowników nie ma zazwyczaj sensu, ze względu na wspomniane wcześniej ograniczenia występujące w przypadku tego rodzaju ataków. Pomimo tego ręczne sprawdzanie wszystkich możliwości metodą manualnej próby logowania do zdalnej usługi nie ma najmniejszego sensu. W skrajnych przypadkach trwałoby to bardzo długo, a po drodze na pewno przydarzyłyby się błędy przy ręcznym wpisywaniu haseł. W konsekwencji cała próba okazałaby się mało wiarygodna i bardzo czasochłonna. Na tym etapie należy więc skorzystać z narzędzia umożliwiającego automatyczne próby logowania do rozmaitych systemów i usług na podstawie zadanej listy haseł.

Okazuje się, że idealne narzędzie do tego celu stworzyła niemiecka grupa hakerów, działająca pod nazwą THC (ang. *The Hacker's Choice*). THC Hydra to program pozwalający na stosunkowo szybkie testowanie haseł do wielu różnych usług. Narzędzie to obsługuje kilkadziesiąt protokołów, z których najważniejsze to:

- telnet,
- ftp,
- http,
- https,
- smb,
- ms-sql,
- mysql,
- rsh,
- snmp,
- vnc,
- pop3,
- imap,
- Cisco auth,
- Cisco enable,
- Cisco AAA.

Myślę, że omawianie wszystkich parametrów programu nie ma sensu. Zamiast tego warto zapoznać się z kilkoma przykładami praktycznego wykorzystania Hydry. Dla każdego z przedstawionych przykładów przyjęte zostało założenie, że lista potencjalnych haseł do atakowanego systemu została wcześniej przygotowana i zapisana w pliku *slownik.txt*.

Załóżmy, że naszym celem jest złamanie hasła do routera Cisco, który wcześniej zidentyfikowaliśmy za pomocą skanera Nmap. Skanowanie wykazało, że urządzenie to pozwala między innymi na nawiązywanie połączeń na 23 porcie TCP, czyli umożliwia tekstowe zarządzanie poprzez protokół telnet. W celu wykonania próby złamania hasła do domyślnego konta o nazwie *cisco*, wystarczy uruchomić Hydrę z następującymi parametrami: *hydra adres_IP_celu telnet -s 23 -v -l cisco -P /slownik.txt -e ns -t 36* (Rysunek 4). Wykorzystany w tym przypadku plik potencjalnych haseł zawierał domyślne hasła spotykane w przypadku urządzeń Cisco oraz kilka najczęściej używanych haseł. Już po kilku sekundach Hydra zakończyła pracę, wyświetlając odnalezione hasło do konta *cisco*. W tym przypadku administrator nie usunął konta domyślnego ani nie zmienił związanego z nim hasła, dzięki czemu udało się ustalić dane umożliwiające intruzowi zalogowanie się do systemu. Jak widać, obsługa Hydry nie jest szczególnie skomplikowana, znaczenie poszczególnych parametrów wywołania jest następujące:

- *telnet* – rodzaj usługi, do której hasła chcemy testować,
- *-s 23* – numer portu,
- *-l cisco* – login, dla którego hasła chcemy testować,
- *-P /slownik.txt* – hasło lub plik z listą haseł, które zamierzamy przetestować,
- *-e ns* – włączenie testowania haseł pustych oraz identycznych z loginem,
- *-t 36* – liczba jednoczesnych połączeń do atakowanej usługi.

Twórcy tego narzędzia do tego stopnia postawili na prostotę obsługi, że stworzyli nawet nakładkę graficzną, zwaną HydraGTK. W tym przypadku atak z przygotowaną wcześniej listą haseł sprowadza się do uzupełnienia odpowiednich pól w kilku zakładkach programu oraz załadowania listy prawdopodobnych haseł. Testując nakładkę graficzną, wykonałem atak na usługę telnet pracującą na drukarce sieciowej firmy HP. Wiedząc, że wbudowane konto nazywa się w tym przypadku *admin*, rozpocząłem atak. Tym razem Hydra ponownie ustaliła dane umożliwiające zalogowanie się do drukarki – okazało się bowiem, że wbudowane konto nie zostało zabezpieczone żadnym hasłem (Rysunek 5).

Kolejny przykład nietuzinkowych możliwości Hydry, jaki chciałbym przedstawić od podstaw, to włamanie do konta poczty elektronicznej dostępnego poprzez protokół pop3. Zakładam, że intruz zna wyłącznie nazwę konta (*jan.tajny* – konto to zostało przeze mnie utworzone w celach testowych) oraz domenę (*o2.pl*). W tym przypadku należy rozpocząć od ustalenia adresu IP serwera pocztowego. Wystarczy w dowolnym systemie operacyjnym wydać polecenie: `ping poczta.o2.pl`. Wynik polecenia powinien zawierać między innymi interesujący nas adres, czyli wartość: 193.17.41.99. Następny, kluczowy, etap to wygenerowanie słownika prawdopodobnych haseł. Załóżmy, że intruz, posiadający wiedzę o typach najczęściej wykorzystywanych haseł, utworzył słownik zawierający następujące potencjalne hasła (wykorzystując wyłącznie wiedzę dotyczącą nazwy konta):

- *jan.tajny*,
- *tajny.jan*,
- *jan.tajny1*,
- *1jan.tajny*,
- *tajny.jan1*,
- *1tajny.jan*,
- *jantajny*,
- *tajnyjan*,
- *jantajny1*,
- *1jantajny*,
- *tajnyjan1*,
- *1tajnyjan*.

Mając przygotowany słownik potencjalnych haseł, wystarczy już tylko uruchomić Hydrę z odpowiednimi parametrami: `hydra 193.17.41.99 pop3 -s 110 -v -l jan.tajny -P /slownik.txt -t 1 -f`. Znaczenie poszczególnych przełączników jest takie samo, jak we wcześniejszym przykładzie. Tym razem jednak atakujemy protokół pop3, czyli port 110/TCP. Nowość stanowi w tym wypadku ograniczenie liczby jednoczesnych prób logowania (można by powiedzieć *głów* hydry) do jednej oraz przełącznik `-f`, wymuszający zakończenie działania po pierwszej udanej próbie zalogowania. Wszystko to ma oczywiście na celu uniknięcie zablokowania próby w wyniku przekroczenia ograniczeń nakładanych przez zdalny serwer na liczbę jednoczesnych oraz powtarzających się w określonym czasie prób logowania. Przy tak dobranym słowniku, już po chwili Hydrze udaje się znaleźć hasło broniące dostępu do konta, co zostaje zasygnalizowane odpowiednim komunikatem:

```
[110] [pop3] host: 193.17.41.99
   login: jan.tajny   password:
      1jan.tajny.
```

Przedstawiłem zaledwie trzy przykłady praktycznego wykorzystania Hydry. Spoglądając jednak na imponującą listę obsługiwanych przez ten program protokołów, łatwo wyobrazić sobie, czego może dokonać wprawny i pomysłowy włamywacz. Program ten umożliwia testowanie stron WWW zabezpieczonych hasłem, obsługuje protokoły szyfrowane, pocztowe oraz bazodanowe, a to tylko niektóre z jego możliwości. Hydra jest więc obecnie jednym z najgroźniejszych narzędzi, po jakie może sięgnąć komputerowy włamywacz. Dobrze byłoby jednak, gdyby Hydrę oswoili również administratorzy systemów komputerowych, gdyż program ten może się okazać nieocenionym narzędziem do wykrywania słabych i potencjalnie niebezpiecznych haseł, pozostawionych gdzieś w zakamarkach administrowanych przez nich urządzeń i programów.

Podsumowanie

Na koniec muszę przestrzec wszystkich Czytelników. Przedstawione metody zdobywania haseł do zdalnych systemów komputerowych można legalnie wykorzystywać wyłącznie do testowania słabości własnych systemów! Uzyskiwanie dostępu do cudzych systemów informatycznych zagrożone jest karą pozbawienia wolności. W żadnym wypadku nie należy więc wykorzystywać przedstawionych procedur w stosunku do obcych sieci i komputerów w nich pracujących.

Mam nadzieję, że udało mi się zwrócić uwagę administratorów na ogromne zagrożenie, jakie stanowi pozostawianie haseł domyślnych oraz konfigurowanie haseł łatwych do odgadnięcia. Testowanie haseł domyślnych oraz profilowanie właścicieli kont w celu utworzenia listy potencjalnie wykorzystywanych przez nich haseł to oczywiście niejedyne metody ataków na hasła do zdalnych systemów. Przykłady innych technik zdobywania haseł „online" stanowią ataki polegające na podsłuchiwaniu uprawnionych transmisji oraz coraz bardziej popularne metody typu *man in the middle*. Jest to już jednak temat na odrębny artykuł.

Należy więc zawsze pamiętać, że komputerowi przestępcy znają ludzkie słabości i bez skrupułów je wykorzystują. Poza tym często są to wysokiej klasy eksperci w dziedzinie technicznych zabezpieczeń informacji. Paradoksalnie, wykorzystywane przez nich narzędzia, takie jak THC Hydra, mogą posłużyć uprawnionym administratorom do obrony przed włamywaczami – dzięki umożliwieniu własnoręcznego testowania słabości zarządzanych systemów.

W Sieci

- *http://nmap.org* – Nmap,
- *http://www.phenoelit-us.org/dpl/dpl.html* – Phenoelit's Default Password List,
- *http://www.cirt.net/cgi-bin/passwd.pl* – CIRT's Default Password List,
- *http://www.virus.org/default-password* – Default Password Database,
- *http://www.openwall.com/passwords/wordlists/password.lst* – najczęściej używane hasła,
- *http://ophcrack.sourceforge.net* – Ophcrack,
- *http://freeworld.thc.org* – The Hacker's Choice Group,
- *http://freeworld.thc.org/thc-hydra* – THC Hydra.

Wojciech Smol
Autor jest absolwentem wydziału Automatyki, Elektroniki i Informatyki Politechniki Śląskiej w Gliwicach. Ukończył studia na kierunku Informatyka, o specjalności Bazy danych, sieci i systemy komputerowe. Pracuje jako administrator sieci i systemów komputerowych w firmie Mostostal Zabrze Holding S.A. Autor nie posiada profilu w serwisie nasza-klasa.pl.
Kontakt z autorem: *wojciech.smol@mz.pl*