

GO H*CK YOURSELF

Proste wprowadzenie
do obrony przed cyberatakami

BRYSON PAYNE



Helion 

Tytuł oryginału: Go H*ck Yourself: A Simple Introduction to Cyber Attacks and Defense

Tłumaczenie: Piotr Ptaszek

ISBN: 978-83-8322-083-3

Copyright © 2022 by Bryson Payne. Title of English-language original: Go H*ck Yourself: A Simple Introduction to Cyber Attacks and Defense, ISBN 9781718502000, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103.

The Polish-language 1st edition Copyright © 2023 by Helion S.A. under license by No Starch Press Inc. All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<https://helion.pl/user/opinie/samsie>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: <https://helion.pl> (księgarnia internetowa, katalog książek)

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

PODZIĘKOWANIA	9
WPROWADZENIE	11
1	
ZABEZPIECZENIE PRZEZ UKRYWANIE	15
Jak przeglądarki „zabezpieczają” hasła	16
Ujawnianie ukrytego hasła	16
Używanie i nadużywanie tego hacka	20
Ochrona haseł	21
Wnioski	22
2	
ATAKI Z DOSTĘPEM FIZYCZNYM	23
Sticky Keys hack	24
Uruchamianie z płyty instalacyjnej systemu Windows 10	24
Uzyskiwanie dostępu na poziomie administratora	27
Teraz jesteś administratorem! Zaloguj się!	29
Mac root hack	31
Aktualizacja ustawień użytkownika root	31
Teraz jesteś użytkownikiem root!	33
Inne fizyczne hacki	33
Ochrona przed atakami fizycznymi	34
Wnioski	34
3	
TWORZENIE WŁASNEGO WIRTUALNEGO LABORATORIUM HAKERSKIEGO	36
Konfiguracja VirtualBox	37
Tworzenie wirtualnej maszyny Kali Linux	37
Uruchamianie maszyny wirtualnej Kali	38
Tworzenie maszyny wirtualnej Windows	40
Podłączanie maszyn wirtualnych do sieci wirtualnej	42
Podłączanie maszyny wirtualnej Kali	42
Podłączanie maszyny wirtualnej z systemem Windows	43

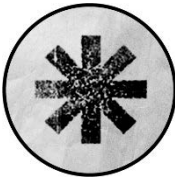
Aktualizowanie systemów operacyjnych maszyn wirtualnych	45
Aktualizowanie systemu Kali Linux	45
Aktualizowanie systemu Windows	46
Wnioski	46
4	
REKONESANS ONLINE I SAMOOBRONA	47
Wygoogluj się (zanim zrobi to Twój wróg)	47
Zaawansowane wyszukiwanie w Google	49
Wyszukiwanie haseł z operatorem ext:	50
Znajdowanie haseł z operatorem site:	53
Baza danych Google Hacking	53
Jak etyczni hakerzy korzystają z Google	55
Media społecznościowe i niebezpieczeństwa związane z nadmiernym udostępnianiem informacji	55
Dane o lokalizacji — niewypowiedziane niebezpieczeństwo mediów społecznościowych	56
Ochrona w mediach społecznościowych	57
Wnioski	58
5	
INŻYNIERIA SPOŁECZNA I ATAKI PHISHINGOWE	59
Jak działa inżynieria społeczna	60
Tworzenie strony phishingowej	60
Klonowanie strony logowania	63
Zbierzmy trochę poświadczeń!	65
Tworzenie wiadomości phishingowej e-mail	67
Ochrona przed atakami phishingowymi	68
Wnioski	69
6	
ZDALNE HAKOWANIE Z MALWARE'EM	70
Tworzenie własnego wirusa	71
Udostępnianie złośliwego oprogramowania	74
Nasłuchiwanie trojana	74
Infekowanie maszyny wirtualnej z systemem Windows	76
Kontrolowanie maszyny wirtualnej z systemem Windows za pomocą Meterpretera	79
Przeglądanie i przesyłanie plików	80
Pobieranie plików z komputera ofiary	83
Wyświetlanie ekranu komputera ofiary	84
Rejestrowanie naciśnięć klawiszy	86
Szpiegowanie przez kamery internetowe	87
Obrona przed złośliwym oprogramowaniem	89
Wnioski	90

7	
KRADZIEŻ I ŁAMANIE HASEŁ	92
Hasze haseł	92
Kradzież haszy haseł systemu Windows	93
Tworzenie użytkowników w systemie Windows	94
Włamanie z powrotem do systemu Windows 10 za pomocą Meterpretera	95
Eskalacja uprawnień	96
Wykradanie haszy haseł za pomocą Mimikatz'a	98
Łamanie haseł	99
Darmowe bazy danych haseł online	100
John the Ripper	101
Używanie bezpieczniejszych haseł	107
Wnioski	109
8	
WEB HACKING	110
Maszyna wirtualna Metasploitable	111
Hakowanie stron internetowych z poziomu przeglądarki	113
Przeprowadzanie ataków typu cross-site scripting	114
Przeprowadzanie ataków typu SQL injection na bazy danych	119
Zabezpieczanie aplikacji internetowych przed XSS, SQLi i innymi atakami	122
Wnioski	124
9	
HAKOWANIE URZĄDZEŃ MOBILNYCH	125
Tworzenie maszyny wirtualnej telefonu/tabletu z Androidem	125
Uruchamianie trojana w systemie Android	128
Infekowanie maszyny wirtualnej z systemem Android	129
Sterowanie maszyną wirtualną z systemem Android	132
Działające aplikacje	133
Dostęp do kontaktów	135
Szpiegowanie przez kamerę	137
Wykradanie plików i szperanie w logach	138
Wyłączanie dzwonka i nie tylko	141
Obrona przed złośliwymi aplikacjami	143
Wnioski	144
10	
HAKOWANIE AUT I INTERNETU RZECZY	145
Instalowanie oprogramowania do hakowania samochodów	146
Przygotowanie wirtualnej sieci magistrali CAN	147
Hakowanie samochodu	149
Przeglądanie pakietów	150
Przechwytywanie pakietów	151

Odtwarzanie pakietów	152
Wysyłanie nowych poleceń	153
Jak napastnicy hakują prawdziwe samochody	155
Wnioski	156
11	
10 RZECZY, JAKIE MOŻESZ ZROBIĆ JUŻ TERAZ, ŻEBY CHRONIĆ SIĘ W INTERNECIE	157
1. Zdaj sobie sprawę, że jesteś celem	157
2. Uważaj na socjotechnikę	158
3. Pamiętaj o znaczeniu bezpieczeństwa fizycznego i w miarę możliwości wyłączaj urządzenia	158
4. Zawsze pomyśl, zanim klikniesz	159
5. Użyj menedżera haseł i włącz uwierzytelnianie dwuskładnikowe	159
6. Aktualizuj swoje oprogramowanie	160
7. Chroń swoje najbardziej wrażliwe dane	161
8. Mądrze korzystaj z oprogramowania zabezpieczającego	162
9. Utwórz kopię zapasową danych, które chcesz zachować	162
10. Porozmawiaj z rodziną	162
Wnioski	163
A	
TWORZENIE PŁYTY INSTALACYJNEJ SYSTEMU WINDOWS 10 LUB PENDRIVE'A	164
Pobieranie systemu Windows 10	165
Nagrywanie systemu Windows 10 na płytę DVD	166
Instalowanie systemu Windows 10 na dysku USB	166
B	
ROZWIĄZYWANIE PROBLEMÓW Z VIRTUALBOX	169
Rozwiązywanie problemów z VirtualBox na Macu	169
Rozwiązywanie problemów z VirtualBox w systemie Windows	170
Wyłącz opcje Hyper-V	170
Włącz wirtualizację w ustawieniach BIOS/UEFI	170
Ostatni problem: niektóre programy antywirusowe	173
SKOROWIDZ	174

1

Zabezpieczenie przez ukrywanie



W TYM ROZDZIALE ZACZNIESZ UCZYĆ SIĘ MYŚLEĆ JAK HAKER, ABY ZNALEŻĆ SŁABE PUNKTY W ŚRODKACH BEZPIECZEŃSTWA. ODKRYJESZ PROSTY HACK DO UJAWNIANIA HASEŁ UKRYTYCH W PRZEGLĄDARCE INTERNETOWEJ. Ten sposób działa, ponieważ przeglądarki internetowe chronią hasła za pomocą *zabezpieczenia przez ukrywanie*.

Zabezpieczenie przez ukrywanie (ang. *security through obscurity*) to technika, w której próbuje się zapewnić bezpieczeństwo czegoś poprzez ukrycie tego. W świecie fizycznym chowanie klucza do domu pod matą powitalną przed drzwiami jest przykładem zabezpieczenia poprzez ukrycie. Twój dom może *wydawać* się bezpieczny, ale to bezpieczeństwo załamuje się, gdy tylko ktoś pomyśli, żeby zajrzeć pod matę.

Ukrywanie czegoś w celu zapewnienia bezpieczeństwa niekoniecznie jest złym podejściem, chyba że jest to *jedyny* środek bezpieczeństwa, jaki został przez Ciebie zastosowany. Niestety, technika zabezpieczenia przez ukrywanie często zawodzi, zwłaszcza gdy jest stosowana na naszych komputerach. Na przykład wielu użytkowników „ukrywa” swoje hasła w dokumencie tekstowym lub arkuszu kalkulacyjnym programu Excel na swoim komputerze lub, co gorsza, na kartce samoprzylepnej pod klawiaturą lub w szufladzie biurka. Te hasła są jeszcze łatwiejsze do znalezienia niż to, które zhakujesz w tym rozdziale. Podobnie niektórzy twórcy oprogramowania na stałe umieszczają ukryte hasła i inne tajne wartości w swoich aplikacjach, ale doświadczony haker często potrafi znaleźć i zdekodować te wartości.

Jak zobaczysz w tym rozdziale, jeśli ukrywanie jest Twoim jedynym zabezpieczeniem, zmotywowany intruz będzie potrzebował do znalezienia drogi do środka wyłącznie odrobiny czasu i energii.

Jak przeglądarki „zabezpieczają” hasła

Kiedy wpisujesz hasło, aby zalogować się do usługi online, takiej jak poczta e-mail lub konto w mediach społecznościowych, Twoja przeglądarka internetowa zwykle ukrywa hasło za pomocą kropek lub gwiazdek. W ten sposób ktoś zagląający Ci przez ramię nie może go odczytać. Jeśli nakażesz przeglądarce, aby zapisała hasło, a później wrócisz do witryny, te kropki lub gwiazdki pojawiają się w polu hasła automatycznie, gdy przeglądarka wprowadzi Twoje zapisane hasło.

Te kropki lub gwiazdki są świetnym przykładem bezpieczeństwa poprzez ukrywanie. Twoja przeglądarka nie szyfruje Twojego hasła ani nie chroni go w żaden inny specjalny sposób. Po prostu zasłania znaki w polu hasła, aby chronić hasło przed przypadkowymi szpiegami. Ta technika wcale nie jest bezpieczna. W rzeczywistości haker potrzebuje tylko kilku sekund przy Twojej klawiaturze, aby zobaczyć hasło.

Ujawnianie ukrytego hasła

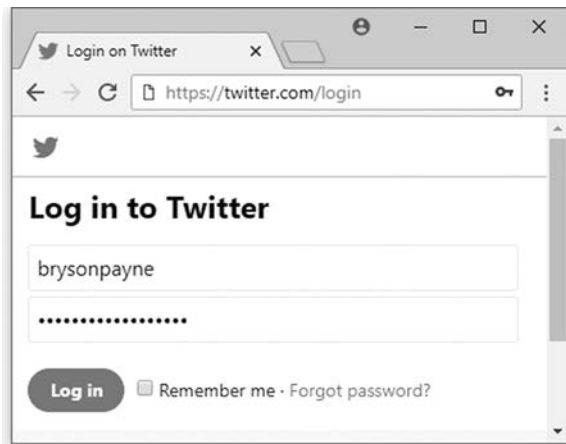
Aby ujawnić hasło ukryte przez przeglądarkę, użyjemy narzędzia Inspect przeglądarki. Narzędzie to umożliwia przeglądanie i tymczasową edycję *kodu źródłowego* strony internetowej, czyli kodu, który mówi przeglądarce, jak wyświetlić stronę internetową. Zmienimy fragment kodu źródłowego, który powoduje, że hasło wyświetla się jako kropki lub gwiazdki. Kiedy skończymy, hasło wyświetli się jako zwykły tekst.

To nie jest rodzaj włamania, który mógłby zniszczyć państwo lub skompromitować prywatne dane milionów ludzi za jednym zamachem. Ten hack ilustruje raczej jedną z głównych zasad hakingu: wykorzystanie istniejącego narzędzia — w tym przypadku narzędzia Inspect przeglądarki — w kreatywny sposób, aby osiągnąć określony cel: ujawnić ukryte hasło. Jednocześnie hack ten ukazuje ryzyko przechowywania haseł w przeglądarce w przypadku, gdy atakujący uzyska fizyczny dostęp do Twojego komputera.

Wypróbujmy ten hack, używając jako przykładu strony logowania Twittera. Wprowadzimy fałszywą nazwę użytkownika i hasło, uruchomimy narzędzie Inspect przeglądarki i zaktualizujemy kod źródłowy, aby ujawnić hasło.

1. Otwórz Google Chrome i przejdź do <https://twitter.com/login/>. Ten hack będzie działał również w innych przeglądarkach, ale dla uproszczenia użyjemy Chrome'a.

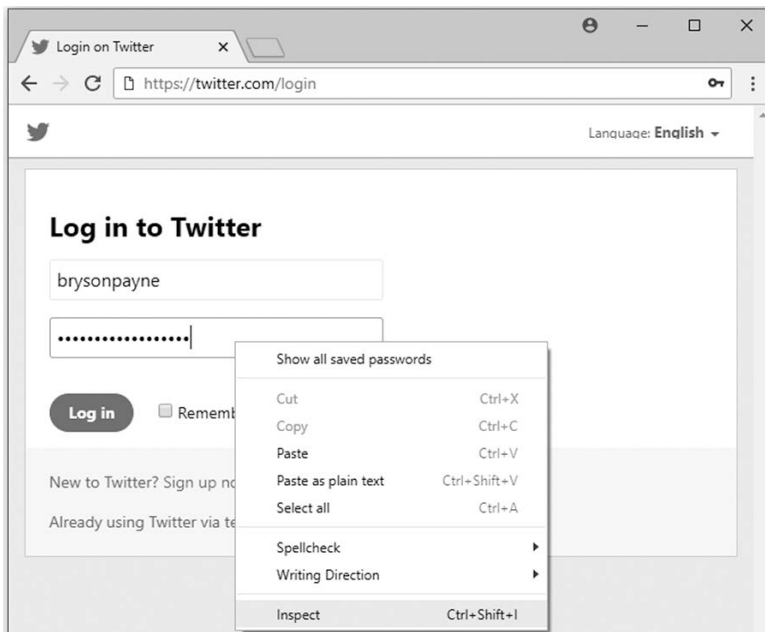
2. Wpisz swoją nazwę użytkownika w polu nazwy użytkownika i **Notmyreal** → **password!** w polu hasła. *Nie* wpisz swojego prawdziwego hasła. Hasło zostanie zasłonięte kropkami, jak pokazano na rysunku 1.1.



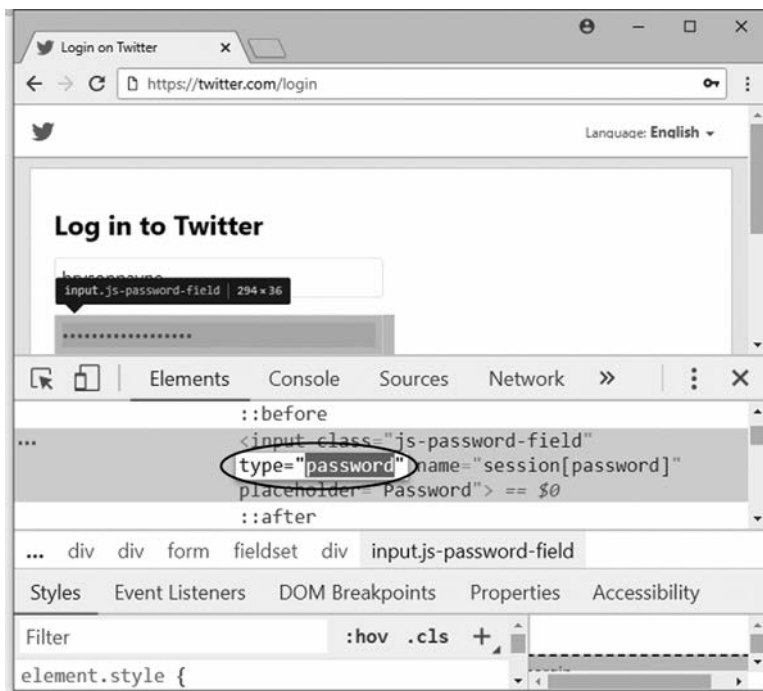
Rysunek 1.1. Przeglądarki internetowe zwykle zasłaniają hasła kropkami lub gwiazdkami

3. Kliknij prawym przyciskiem myszy (lub kliknij z wciśniętym klawiszem *Ctrl* na komputerze Mac) pole hasła i wybierz *Inspect*, jak pokazano na rysunku 1.2. W przeglądarce powinno otworzyć się narzędzie *Inspect*, które będzie zestawem okien pokazujących kod. Ponieważ kliknąłeś (kliknęłaś) prawym przyciskiem myszy pole hasła, aby otworzyć narzędzie *Inspect*, przeglądarka powinna już podświetlać część kodu, która tworzy pole hasła na stronie logowania.
4. Znajdź `type="password"` w podświetlonym kodzie i kliknij dwukrotnie słowo `password`, aby je zaznaczyć, jak pokazano na rysunku 1.3. Ten fragment kodu określa sposób, w jaki przeglądarka identyfikuje pole hasła. Przeglądarka rozpoznaje, że każdy tekst w polu o typie `password` powinien być zasłonięty.
5. Po podświetleniu `password` naciśnij spację, aby zastąpić to słowo spacją (`type=" "`), jak pokazano na rysunku 1.4. Teraz zmieniliśmy (lub zhakowaliśmy) kod pola hasła tak, aby przeglądarka nie rozpoznawała, że ma to być pole z hasłem. Powinno to ujawnić dowolny tekst w polu hasła!

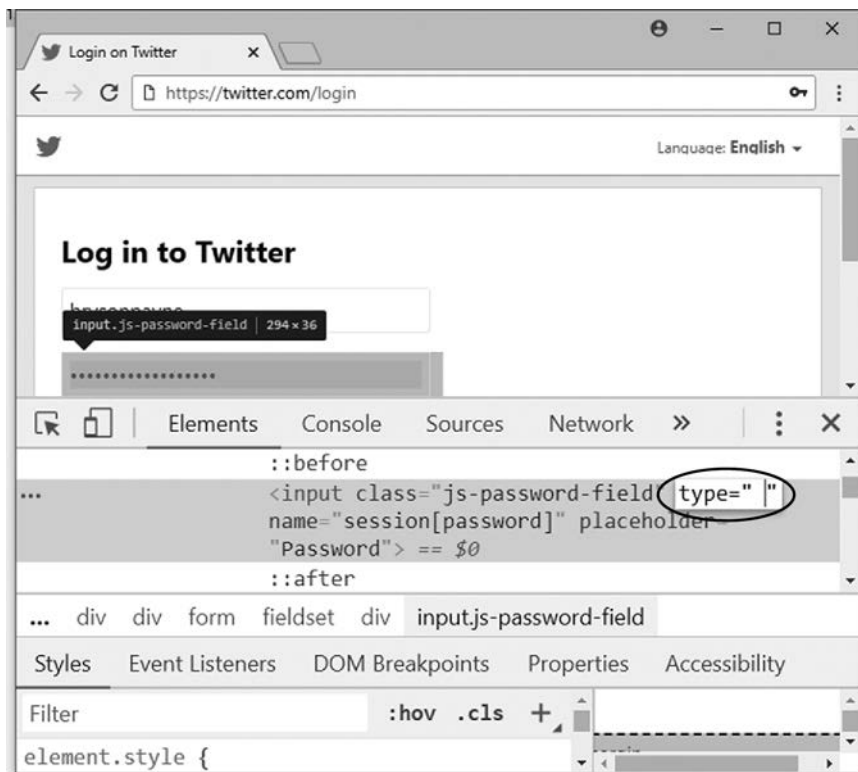
UWAGA *Ten hack nie ma wpływu na sam Twitter. Po prostu zmienia sposób, w jaki przeglądarka na Twoim komputerze wyświetla stronę logowania Twittera.*



Rysunek 1.2. Inspekcja kodu hasła



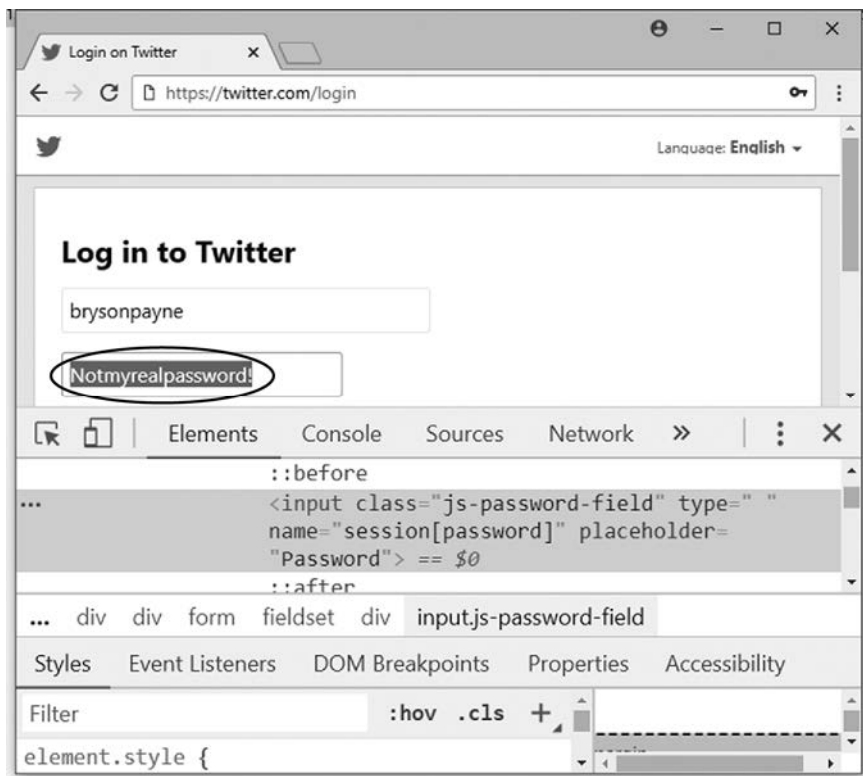
Rysunek 1.3. Znalezienie `type="password"` w narzędziu Inspect



Rysunek 1.4. Zamiana słowa `password` na `type="password"`

- Naciśnij *Enter*, aby wyświetlić zaktualizowany kod w przeglądarce. Powinieneś (powinnaś) teraz zobaczyć wpisane hasło jako zwykły tekst w oknie przeglądarki, jak pokazano na rysunku 1.5.

Ten hack zadziałał, ponieważ tag `<input>`, który pozwala twórcom stron internetowych tworzyć pola haseł, jest niezabezpieczony — i to już od ćwierć wieku. W latach 90. XX wieku, kiedy pierwsi twórcy stron internetowych dodali tag `<input>` do *HyperText Markup Language (HTML)*, języka, który umożliwił wyświetlanie stron internetowych w przeglądarkach internetowych, ich jedynym zabezpieczeniem było zastępowanie znaków hasła kropkami lub gwiazdkami za pomocą dodatkowego kodu `type="password"`. Jednakże, ponieważ zwykłe pola tekstowe również używają tagu `<input>`, możemy zastosować narzędzie *Inspect* do zmiany wprowadzonego hasła na zwykłe wprowadzanie tekstu, po prostu zmieniając `type="password"` na `type=" "`.



Rysunek 1.5. Hasło jest teraz widoczne

Używanie i nadużywanie tego hacka

Hack, który właśnie wypróbowaliśmy, ma praktyczne, etyczne zastosowania. Ponieważ hasła przechowywane w przeglądarce są automatycznie wypełniane, ale ukryte na ekranie logowania do witryny, możesz użyć tego prostego hacka do tego, aby zdemaskować hasło, którego zapomniałeś(-łaś). Jest to szczególnie przydatne, jeśli przechowujesz swoje hasła na jednym komputerze, na przykład komputerze domowym, ale okresowo musisz logować się z innych urządzeń, takich jak komputer służbowy, komputer członka rodziny lub urządzenie mobilne. Jeśli nie pamiętasz swojego hasła, gdy próbujesz zalogować się na innym komputerze, możesz zdemaskować zapisane hasło na komputerze domowym, aby je sprawdzić, zamiast je zresetować.

Ten hack może być również używany etycznie na inne sposoby. Na przykład jeśli pracownik niespodziewanie opuszcza firmę, etyczny haker za zgodą właściciela firmy może użyć tego hacka, aby odzyskać hasła do ważnych kont internetowych, za które pracownik ten mógł być odpowiedzialny.

Jeśli przećwiczysz to wystarczająco dużo razy, możesz z łatwością wykonać ten hack w mniej niż pięć sekund. Oznacza to jednak również, że jeśli kiedykolwiek będziesz przechowywać hasło na komputerze publicznym, każda osoba z fizycznym dostępem do tego komputera będzie potrzebować tylko pięciu sekund, aby je ukraść. Haker w czarnym kapeluszu (ang. *black hat hacker*) może wejść do hotelowego lobby lub biblioteki publicznej prawie w dowolnym miejscu na świecie, usiąść przy komputerze, sprawdzić historię przeglądarki pod kątem ostatnio odwiedzanych stron internetowych i przekonać się, czy potencjalne ofiary zapisały swoje hasła podczas logowania na swoje prywatne konta.

Nie musisz nawet zapisywać swojego hasła w przeglądarce, aby ktoś je ujawnił. Jeśli jesteś w miejscu publicznym i ktoś odciągnie Cię od komputera podczas wpisywania hasła na stronie internetowej, może użyć tego hacka do kradzieży Twojego hasła. Może nawet naprawić kod `type="password"` i zamknąć narzędzie Inspect, aby zatrzeć ślady! Jeśli użyłeś(-łaś) tego samego hasła do wielu kont, atakujący będzie teraz w stanie uzyskać dostęp do nich wszystkich.

Ochrona haseł

Omawiany przez nas hack, gdy jest wykorzystywany w sposób złośliwy, stanowi wyraźne zagrożenie dla bezpieczeństwa Twoich haseł. Istnieje jednak kilka prostych sposobów, dzięki którym możesz się chronić. Ten hack jest możliwy tylko wtedy, gdy haker ma fizyczny dostęp do przechowywanych haseł, więc kluczem do uniemożliwienia ataku jest nieprzechowywanie haseł w przeglądarce albo wprowadzenie pewnych ograniczeń:

- **Miejsce przechowywania haseł.** Przechowuj hasło w przeglądarce tylko na komputerze lub urządzeniu, które posiadasz i trzymasz przy sobie, nigdy na komputerze publicznym.
- **Jakie hasła przechowujesz.** Nigdy nie przechowuj swojego hasła do poczty elektronicznej, ponieważ osoba atakująca może zazwyczaj odkryć lub zresetować wszystkie inne Twoje hasła za pomocą konta e-mail.
- **Kto ma dostęp do Twojego komputera.** Trzymaj komputer przy sobie lub w bezpiecznym miejscu i nie zostawiaj go otwartego, jeśli musisz odejść, nawet na minutę.

Jeśli musisz połączyć się z prywatnym kontem z komputera publicznego, ogranicz informacje przechowywane w przeglądarce, używając trybu incognito (*Ctrl+Shift+N*) w przeglądarce Chrome lub otwierając nowe okno prywatne w przeglądarce Firefox (*Ctrl+Shift+P*) albo Safari (*Shift+⌘+N*). Pamiętaj, aby po zakończeniu sesji wylogować się i całkowicie zamknąć przeglądarkę. Nawet jeśli się wylogujesz lub użyjesz trybu incognito, współużytkowane komputery będą zagrożone ryzykiem, ponieważ złośliwe oprogramowanie może rejestrować Twoje naciśnięcia klawiszy lub inne informacje. (W rzeczywistości przechwycimy naciśnięcia klawiszy za pomocą wirusa, który stworzymy w rozdziale 6.).

Loguj się na konta z komputera publicznego tylko wtedy, gdy jest to absolutnie konieczne. Pomyśl także o zmianie haseł po powrocie do własnego komputera.

Jeśli korzystasz z komputera osobistego w miejscu publicznym, pamiętaj o wylogowaniu się lub zablokowaniu ekranu, gdy odchodzisz — albo jeszcze lepiej, miej komputer przy sobie. Ustaw ekran blokady lub wygaszacz ekranu tak, aby włączał się już po kilku minutach, co ograniczy czas, przez jaki komputer jest narażony na atak, na wypadek gdybyś zapomniał(a) go sam(a) zablokować. Korzystaj z silnego hasła lub frazy hasła (spróbuj użyć czterech lub więcej słów) do logowania się do swojego komputera, zamiast z czegoś oczywistego, jak *password123*, aby inni nie mogli łatwo odblokować Twojego komputera, jeśli będzie on pozostawiony bez dozoru.

Oprócz tych środków powinieneś (powinnaś) skorzystać z innych narzędzi zabezpieczających hasła, takich jak uwierzytelnianie dwuskładnikowe i menedżer haseł, na przykład KeePass, Dashlane, LastPass lub podobny. Omówimy te narzędzia w rozdziale 11.

Ochrona przed atakami komputerowymi wymaga zachowania kilku sprytnych środków ostrożności, ale ważne jest, aby wiedzieć, jak wyważyć wygodę i bezpieczeństwo. Przechowywanie wszystkich haseł do wszystkiego w przeglądarce wydaje się wygodne, ponieważ nigdy nie trzeba ich wpisywać, ale oznacza to również, że każdy, kto ma dostęp do tego komputera, może wykraść Twoje hasła i konta. Musimy znaleźć odpowiednią równowagę między wygodą a bezpieczeństwem, zarówno w świecie fizycznym, jak i w Internecie.

Wnioski

W tym rozdziale przekonałeś(-łaś) się, że bezpieczeństwo poprzez ukrycie nie jest skuteczne. Nauczyłeś(-łaś) się, jak w ciągu kilku sekund ujawnić hasło wprowadzone do przeglądarki, wykonując zaledwie kilka kroków. Dowiedziałeś(-łaś) się również, jak ważne jest, aby nigdy nie przechowywać hasła na komputerze publicznym lub współużytkowanym. Ponadto wiesz już, jak fizycznie chronić swój komputer przed osobami, których nie znasz lub którym nie ufasz — jeśli ktoś może dotknąć Twojej klawiatury, może zarazem uzyskać dostęp do Twoich poufnych informacji.

Omówiony w tym rozdziale hack był przykładem włamania z fizycznym dostępem — aby go wykonać, atakujący potrzebuje fizycznego dostępu do Twojego komputera. W następnym rozdziale poznasz inne hacki z dostępem fizycznym, które pozwalają hakerom na uzyskanie plików z dysku twardego, bez konieczności znajomości danych logowania.

Skorowidz

A

- administrator, 138
- Android, 125
- aplikacje internetowe
 - DVWA, 114
 - zabezpieczanie, 122
- atak
 - phishingowy, 47, 60, 67
 - ochrona, 68
 - słownikowy, 102
 - typu
 - cross-site scripting, 114
 - reflected cross-site scripting, 115
 - SQL injection, 119
 - stored cross-site scripting, 117
 - z dostępem fizycznym
 - Mac root hack, 31
 - ochrona, 34
 - Sticky Keys hack, 24
 - z maską, 104
- atakowanie baz danych, 120

B

- backdoor, 84
- baza danych
 - Google Hacking, 53
 - hasel, 100
- bezpieczeństwo hasel, 107

D

- dane o lokalizacji, 56
- dostęp
 - do kontaktów, 135
 - do wiersza poleceń, 26
 - do wrażliwych informacji, 132
 - na poziomie administratora, 27
- DVWA, 114

E

- eskalacja uprawnień, 96
- exploit, 71

F

- funkcje haszujące, 93

G

- Google
 - hacking, 49
 - Hacking Database, 53
 - Play Protect, 130

H

- hakowanie
 - Internetu rzeczy, 145
 - samochodów, 149
 - hakerzy samochodowi, 155
 - magistrala CAN, 147
 - odtworzenie pakietów, 152
 - oprogramowanie, 146
 - panel sterowania CANBus, 149
 - przechwytywanie pakietów, 151
 - wysyłanie nowych poleceń, 153
 - stron internetowych, 113
 - urządzeń mobilnych, 125
- hasła
 - bezpieczeństwo, 107
 - darmowe bazy danych, 100
 - hasze, 92
 - łamanie, 99
 - atak słownikowy, 102
 - atak z maską, 104
 - ochrona, 21
 - ujawnianie, 16
 - ukrywanie, 16
 - wykradanie haszy, 93, 98
 - wyszukiwanie w Google, 50, 53

I
ICSim, 146, 148
Internet rzeczy, Internet of things, 145
inżynieria społeczna, 60

J
język
 HTML, 115
 JavaScript, 115
John the Ripper, 101

K
Kali Linux, 37
klonowanie strony, 63
kradzież haszy haseł, 93, 98
kryptograficzna funkcja skrótu, 92

L
luka fodhelper, 96

ł
łamanie haseł, 99

M
Mac root hack, 31
maska hasła, 107
maszyna wirtualna Android, 125
 dostęp
 do kontaktów, 135
 do wrażliwych informacji, 132
 infekowanie, 129
 kontrolowanie zdalne, 132
 odczytywanie logów, 138
 szpiegowanie przez kamerę, 137
 tworzenie, 125
 uruchamianie
 aplikacji, 133
 trojana, 128
 wykradanie plików, 138
 wyłączanie dzwonka, 141
maszyna wirtualna Kali, 37
 aktualizowanie systemu, 45
 podłączanie do sieci wirtualnej, 42
 tworzenie, 37
 tworzenie wirusa, 71
 uruchamianie, 38
maszyna wirtualna Metasploitable, 111

maszyna wirtualna Windows, 40
 aktualizowanie systemu, 46
 eskalacja uprawnień, 96
 infekowanie, 76
 kontrolowanie zdalne, 79, 95
 kradzież haszy haseł, 93
 pobieranie plików, 83
 podglądanie kamery internetowej, 87
 podłączanie do sieci wirtualnej, 43
 przesyłanie trojanów, 80
 rejestrowanie naciśnień klawiszy, 86
 tworzenie, 40
 tworzenie użytkowników, 94
 wyświetlanie ekranu, 84
media społecznościowe
 ochrona, 57
 udostępnianie informacji, 55
metadane obrazu, 57
Metasploit Framework, 71
Metasploitable, 111
Meterpreter
 kontrolowanie maszyny wirtualnej, 79, 95
 ponowne łączenie, 133
Mimikatz
 wykradanie haszy haseł, 98

N
narzędzie
 cansniffer, 150
 can-utils candump, 151
 John the Ripper, 101
 msfvenom, 73
nurkowanie na śmietniku, 105

O
ochrona
 aplikacji internetowych, 122
 haseł, 21
 przed
 atakami fizycznymi, 34
 atakami phishingowymi, 68
 zagrożeniami, 157
 złośliwym oprogramowaniem, 89
 złośliwymi aplikacjami mobilnymi, 143
 w mediach społecznościowych, 57
operator
 ext:, 50
 site:, 53

P

- plyta instalacyjna Windows
 - tworzenie, 164
 - uruchamianie systemu, 24
- program
 - cmd.exe, 27
 - fodhelper.exe, 96
 - ICSIm, 146, 148
 - sethc.exe, 27
- przeglądarka metadanych obrazu, 56
- przeglądarki internetowe
 - ukrywanie haseł, 16

R

- rekonesans, 47

S

- SET, Social Engineering Toolkit, 60–66
- sieć wirtualna
 - typu host-only, 42
 - VCAN, 147
- sniffer, 150, 151
- Sticky Keys hack, 24
- strona logowania
 - klonowanie, 63
- strony phishingowe, 60
- superużytkownik, 138

T

- trojan, 128
 - zdalnego dostępu, 71
- tworzenie
 - sieci wirtualnej, 42
 - strony phishingowej, 60
 - wiadomości phishingowej e-mail, 67
 - wirtualnej maszyny, 37, 40
 - własnego wirusa, 71

U

- udostępnianie złośliwego oprogramowania, 74
- ujawnianie ukrytego hasła, 16
- ukrywanie hasła, 16
- urządzenia IoT, 145

- użytkownik
 - administrator, 27, 29
 - root, 31, 33

V

- VirtualBox
 - konfiguracja, 37
 - maszyna wirtualna
 - Android, 125
 - Kali Linux, 37
 - Metasploitable, 111
 - Windows, 40
 - rozwiązywanie problemów, 169
 - sieć typu host-only, 42
- VirusTotal, 49, 51

W

- web hacking, 110
- wiadomość phishingowa e-mail, 67
- Windows 10
 - tworzenie płyty instalacyjnej, 164
- Windows Defender, 77
- wirtualna sieć magistrali CAN, VCAN, 147
- wstrzykiwanie kodu, 115, 119
- wyłączanie
 - Google Play Protect, 130
 - Windows Defendera, 77
 - zapory systemu Windows, 77
- wyszukiwarka Google, 49
 - operator ext., 50
 - operator site., 53
 - zaawansowane wyszukiwanie, 49

Z

- zabezpieczenie przez ukrywanie, 15
- zapora systemu Windows, 77
- złośliwe oprogramowanie
 - infekowanie, 76
 - nasłuchiwanie trojana, 74
 - obrona, 89, 143
 - tworzenie, 71, 128
 - udostępnianie, 74
 - uruchamianie trojana, 128
- znaki specjalne, 108

PROGRAM PARTNERSKI

— GRUPY HELION —

1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

OSTRZEŻENIE: Ta książka nie może być wykorzystywana do włamywania się na komputery rządowe, niszczenia stron internetowych, dokonywania oszustw phishingowych, kradzieży i łamania haseł, rozpowszechniania wirusów ani jakichkolwiek innych nielegalnych działań.

Hakowanie? Jest prostsze, niż myślisz!

Hakowanie nie zawsze musi być złe. Terminem tym określa się również sprytnie sposoby używania sprzętu czy oprogramowania do czegoś nowego. Z kolei etyczne hakowanie polega na zastosowaniu technik ataków do testowania systemu komputerowego, aby znaleźć jego słabe punkty, usunąć je i w ten sposób wzmocnić jego bezpieczeństwo. Opanowanie metod, jakimi posługują się cyberprzestępcy, pozwala zatem zrozumieć naturę zagrożeń w cyfrowym świecie i skutecznie się przed nimi bronić.

Dzięki tej książce przekonasz się, że typowe ataki hakerskie są bardzo łatwe do wykonania. Zaczynasz od przygotowania wirtualnego laboratorium, w którym bezpiecznie możesz wypróbować różnego rodzaju techniki, nie narażając przy tym nikogo na ryzyko. Następnie krok po kroku będziesz się uczyć przeprowadzać najważniejsze rodzaje ataku, w tym włamania z dostępem fizycznym, Google hacking, ataki phishingowe, socjotechniczne i za pomocą złośliwego oprogramowania, hakowanie stron internetowych, łamanie haseł, wreszcie włamania

do telefonów i samochodów. Dowiesz się, jak prowadzić rekonesans. Przyjrzyś się cyberatakam z punktu widzenia zarówno napastnika, jak i ofiary. Co najważniejsze, wszystkie techniki zostały przedstawione na bazie rzeczywistych przykładów i opatrzone praktycznymi wskazówkami dotyczącymi obrony. W efekcie nie tylko zrozumiesz zasady ataku, ale także poznasz sposoby, jak się ustrzec przed hakerami.

Naucz się hakować, by skutecznie chronić się przed cyberatakami:

- Przeciwicz techniki hakarskie w bezpiecznym, wirtualnym środowisku
- Opanuj obsługę takich narzędzi jak Kali Linux, Metasploit i John the Ripper
- Dowiedz się, na czym polega infekowanie urządzenia złośliwym oprogramowaniem
- Poznaj metody phishingu: wykradanie i łamanie hasła, wyłudzenie poufnych informacji

Dr Bryson Payne — naukowiec, wykładowca, wielokrotnie nagradzany szkoleniowiec i autor książek, niekwestionowany autorytet w dziedzinie bezpieczeństwa, specjalista z wieloletnim doświadczeniem. Zdobył wiele elitarnych certyfikatów, w tym CISSP, CEH, SANS/GIAC GPEN, GRID i GREM. Od ponad 36 lat zajmuje się programowaniem, hakowaniem i inżynierią wsteczną oprogramowania.

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!



ISBN 978-83-8322-083-3



9 788383 220833

Cena: 49,90 zł