GO H*CK YOURSELF

Proste wprowadzenie do obrony przed cyberatakami

BRYSON PAYNE

no starch press

Helion

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

Tłumaczenie: Piotr Ptaszek

ISBN: 978-83-8322-083-3

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/samsie
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

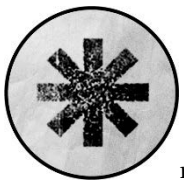
Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

1

Zabezpieczenie przez ukrywanie



W TYM ROZDZIALE ZACZNIESZ UCZYĆ SIĘ MYŚLEĆ JAK HAKER, ABY ZNALEŹĆ 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 potrzebować 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 zaglądający Ci przez ramię nie może go odczytać. Jeśli nakażesz przeglądarce, aby zapisała hasło, a później wrócisz do witryny, te kropki lub gwiazdki pojawią 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

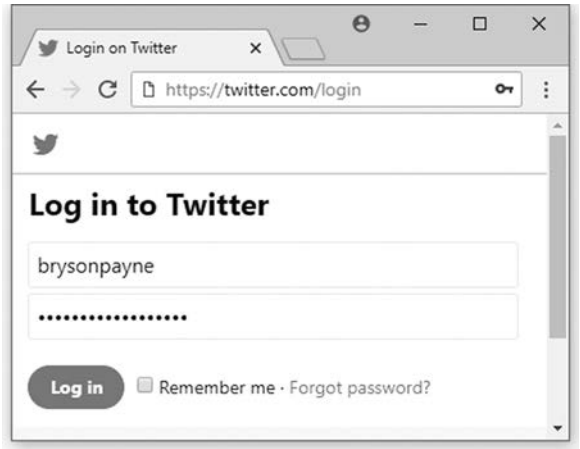
Aby ujawnić hasło ukryte przez przeglądarkę, użyjemy narzędzia Inspect przeglądarki. Narzędzie to umożliwia przeglądanie i tymczasową edycję *kodu źródłowego* strony internetowej, czyli kodu, który mówi przeglądarce, jak wyświetlić stronę internetową. Zmienimy fragment kodu źródłowego, który powoduje, 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.

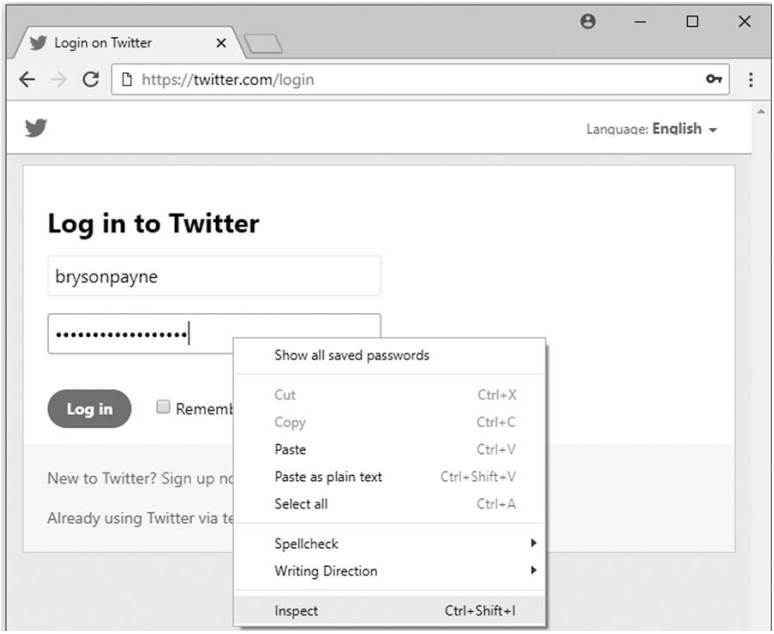
2. Wpisz swoją nazwę użytkownika w polu nazwy użytkownika i **`Notmyreal`**
`↪password!` w polu hasła. *Nie* wpisuj swojego prawdziwego hasła. Hasło zostanie zasłonięte kropkami, jak pokazano na rysunku 1.1.



Rysunek 1.1. Przeglądarki internetowe zwykle zasłaniają hasła kropkami lub gwiazdkami

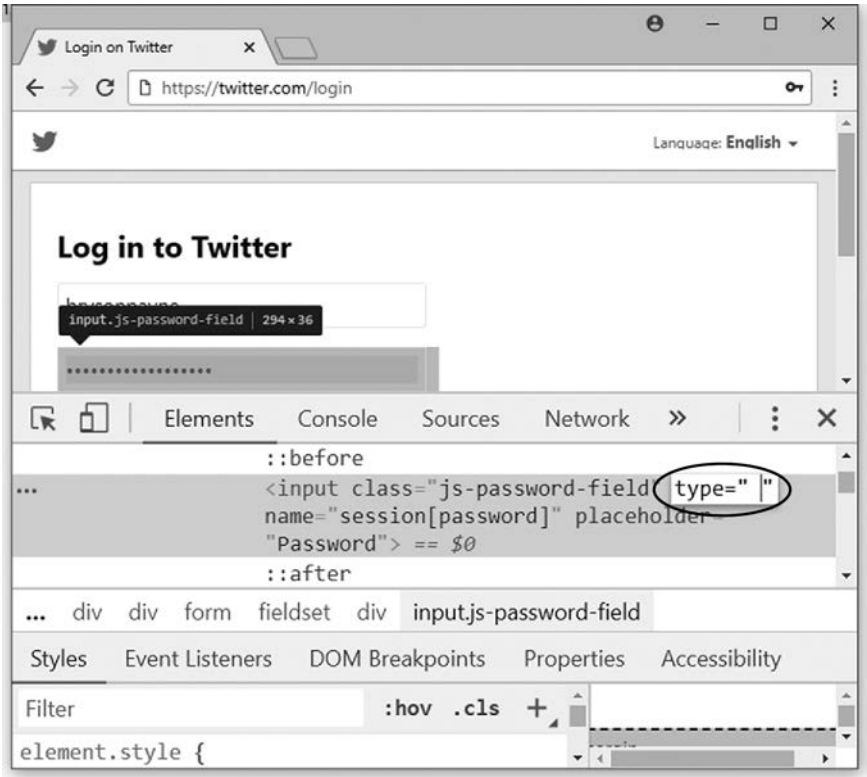
3. Kliknij prawym przyciskiem myszy (lub kliknij z wciśniętym klawiszem *Ctrl* na komputerze Mac) pole hasła i wybierz *Inspect*, jak pokazano na rysunku 1.2. W przeglądarce powinno otworzyć się narzędzie Inspect, które będzie zestawem okien pokazujących kod. Ponieważ kliknąłeś (kliknęłaś) prawym przyciskiem 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

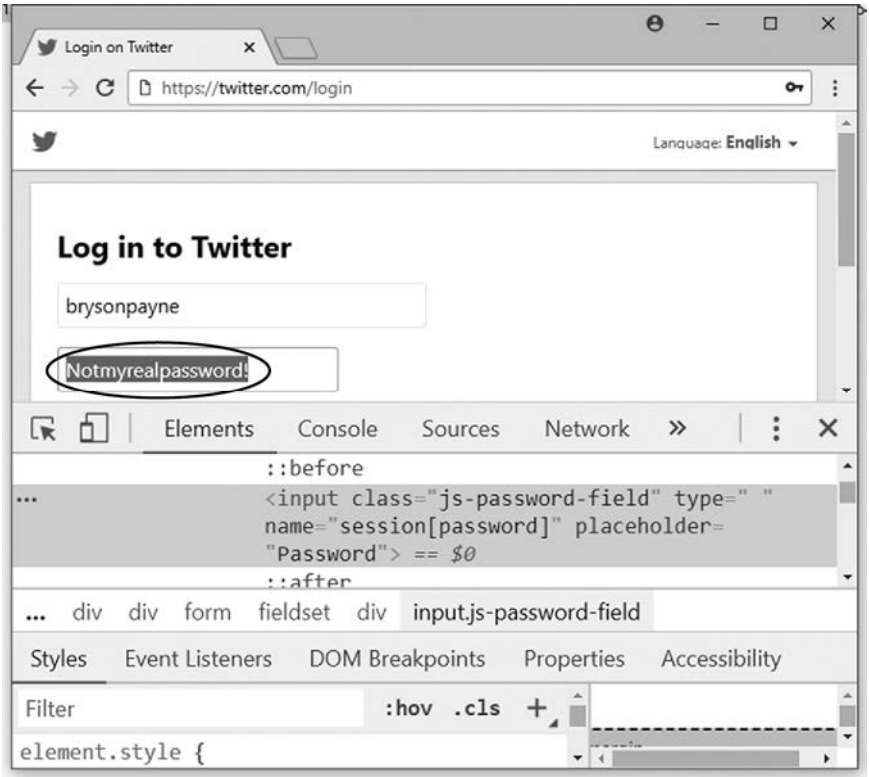
Rysunek 1.3. Znalezienie type="password" w narzędziu Inspect



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

6. 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 umożliwia 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


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 sprytne 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. Zaczniesz od przygotowania wirtualnego laboratorium, w którym bezpiecznie możesz wypróbowywać 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. Przyjrzysz się cyberatakom 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:

- Przećwicz techniki hakerskie 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, wyłudzanie 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