

Wojciech Ciemski

CYBERSECURITY

w pytaniach i odpowiedziach



Helion 

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.

Redaktor prowadzący: Szymon Sz wajger

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą Shutterstock.com.

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)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

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

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-9924-2

Copyright © Helion S.A. 2023

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

Słowo wstępne	11
Wprowadzenie	13
Systemy operacyjne	17
Jaka jest różnica między konteneryzacją a wirtualizacją? Jakie są ich zalety oraz wady w kontekście bezpieczeństwa?	17
Jakie rodzaje baz danych można wskazać?	18
Kto może modyfikować plik z uprawnieniami 777?	19
Czym jest hardening i czego dotyczy?	19
Po co stosuje się dowiązanie symboliczne i czym ono jest?	20
Jaka jest różnica pomiędzy uwierzytelnianiem a autoryzacją?	20
Czym są Kerberos, AD oraz GPO?	20
Czym jest Crypto API?	21
Co znajduje się w plikach /etc/passwd i /etc/shadow?	21
Czym są zmienne środowiskowe?	23
Czy FTP jest bezpieczniejszy niż SSH?	24
Jak za pomocą komendy stworzyć nowy katalog na dysku?	24
Jak wyświetlić zawartość pliku za pomocą komendy?	25
Czym jest serializacja?	25
Jak stworzyć ukryty plik/katalog w systemie?	25
Czym różni się konto root od zwykłego konta użytkownika?	26
Jak wyświetlić listę plików w katalogu?	26
Do czego służy cron? W jakich lokalizacjach znajdują się poszczególne pliki?	27
Czym jest Docker?	27
Do czego wykorzystuje się protokół RDP?	27
Czy projekty open source są bezpieczniejsze od zamkniętych rozwiązań?	28
Jak wyświetlić listę uruchomionych procesów?	28

Do czego służą Wget i cURL?	28
Jaka jest różnica pomiędzy bind shell a reverse shell?	29
Jak można wykorzystać program grep?	29
Na jakiej stronie można sprawdzić, jak wyglądały strony w przeszłości?	30
Sieci	31
Czym jest ARP?	31
Jaka jest różnica pomiędzy routerem a switchem?	31
Jaka jest różnica między rozwiązaniami firewall a WAF?	32
Jaka jest różnica między adresem IP a adresem MAC?	32
Jaka jest różnica między publicznym a prywatnym adresem IP?	33
Jaka jest różnica pomiędzy portem zamkniętym a filtrowanym?	34
Jakie standardowe usługi znajdują się pod portami o numerach: 21, 22, 23, 25, 80, 88, 53, 143, 443, 1433, 1863, 3306, 3389?	34
Jaka jest różnica pomiędzy TCP a UDP?	35
Po co używa się VLAN-ów?	36
Po co używa się zapory sieciowej?	36
Czym jest ping? Czy warto go wyłączyć w organizacji i dlaczego?	36
Jakie warstwy ma model ISO/OSI?	37
Jakie warstwy ma model TCP/IP?	38
Jakim narzędziem można przechwycić pakiety?	38
Co można znaleźć za pomocą Certificate Transparency Log?	39
Co oznacza skrót LAN?	39
Gdzie kieruje adres 127.0.0.1?	39
Do czego używa się adresów 1.1.1.1 i 8.8.8.8?	39
Do czego służy maska podsieci?	40
Do czego służy DHCP?	40
Co to jest DNS i jak działa?	40
Czym jest TCP handshake?	41
Do czego służy komenda tracert/ traceroute?	41

Aplikacje webowe	43
Jaką przewagę nad ciasteczkami mają tokeny JWT?	43
Jaki nagłówek służy do przesyłania ciasteczek?	43
Jaka jest różnica między metodami POST i GET?	44
Jaka jest różnica pomiędzy HTTP a HTML?	44
Jakie znasz kody i klasy odpowiedzi HTTP?	44
Jakim znakiem rozdziela się parametry w żądaniu GET?	51
Czemu strony korzystają z nagłówka HSTS?	51
Jaka wartość znajduje się w nagłówku X-Forwarded-For?	51
Czego można się dowiedzieć o żądaniu na podstawie nagłówka Content-Length?	52
Do czego wykorzystuje się protokół WebSocket?	52
Przed czym chroni CSP?	52
Czym różni się HTTP/2 od HTTP/1.1?	53
Jakie znasz metody HTTP?	54
Co oznacza, że HTTP jest protokołem bezstanowym?	54
O czym informuje zawartość nagłówka User-Agent?	55
Jak wygląda przykładowy plik w formacie JSON?	55
Jak sprawdzić, czy parametr jest podatny na atak path traversal?	56
Na czym polega mechanizm Same-Origin Policy?	56
W jakim celu stosuje się mechanizm CAPTCHA?	56
Przed czym chroni mechanizm prepared statement?	57
Przed czym może chronić atrybut SameSite dodawany do ciasteczek?	57
Z jakich elementów składa się żądanie HTTP?	57
Czy powinno się ustawiać flagę HTTPOnly/Secure w ciasteczkach i dlaczego tak lub nie?	58
Dlaczego po zalogowaniu strony internetowe zwracają ciasteczko?	58
Kryptografia	59
Jakie informacje znajdują się w certyfikacie SSL?	59
MD5 czy SHA-256 — co jest lepsze i dlaczego?	59
Jakie znasz metody szyfrowania?	60

Kiedy mamy do czynienia z kolizją w kontekście kryptografii?	61
Kiedy stosuje się szyfr blokowy, a kiedy szyfr strumieniowy?	61
Jakiej minimalnej długości powinno być hasło użytkownika?	61
Jaka jest różnica pomiędzy haszowaniem a szyfrowaniem?	62
Po co stosujemy funkcje skrótu?	62
Co zapewnia kod HMAC?	62
Czy jest jakaś różnica pomiędzy SSL a TLS?	63
Jaka jest przewaga kryptografii krzywych eliptycznych nad RSA?	63
Do czego można użyć klucza publicznego?	63
Jak zdefiniować salting i do czego jest on używany?	64
Do czego służą sól i pieprz w kontekście haszowania haseł?	64
Co oznacza utajnianie z wyprzedzeniem?	64
Czym różni się zaufany certyfikat SSL od niezaufanego? Po co nam zaufane główne urzędy certyfikacji?	65

Cyberbezpieczeństwo67

Jaka jest różnica pomiędzy podatnością 0-day a 1-day?	67
Czym jest botnet?	67
Jakie mogą być skutki ataku XSS?	67
Jakie znasz rodzaje wstrzyknięć?	68
Po co istnieją numery CVE i do czego służą?	70
Czym zajmują się red team, blue team i purple team?	70
Czym jest triada CIA i z czego się składa?	71
Jakie znasz rodzaje ataków typu sniffing i jak one przebiegają?	72
Na czym polega atak MITM?	72
Czym są SIEM, EDR i UEBA?	72
Czy podatność open redirection jest niebezpieczna?	73
Co jest przyczyną błędów typu buffer overflow?	73
Czy można przeprowadzać test penetracyjny bez pozwolenia?	74
Do czego służy hashcat?	74
Czy można namierzyć osobę, która korzysta z trybu prywatnego w przeglądarce?	75

Do czego używa się MITRE ATT&CK?	75
Czym jest modelowanie zagrożeń?	76
Do czego wykorzystuje się tęczowe tablice?	76
Czym jest exploit?	77
Czym jest DAST?	77
Na czym polega zasada najmniejszego uprzywilejowania?	78
Jakie widzisz różnice pomiędzy DDoS a DoS?	78
Co oznacza pojęcie „insider threat”?	78
Jakie znasz metodyki prowadzenia testów penetracyjnych?	79
Czym charakteryzują się testy black box, grey box i white box?	80
Dlaczego każdy program bug bounty ma zakres? Do czego on służy?	80
Czym są honeypoty i honeynety? Do czego można je wykorzystać?	81
Gdzie można znaleźć informacje o gotowych exploitach?	81
Do czego wykorzystuje się narzędzie nmap?	81
Czym jest cyber kill chain?	82
Czym są podatności typu IDOR?	83
Czym jest steganografia?	84
Co powinien zawierać raport z pentestu?	84
Po co przeprowadza się skanowanie portów?	85
Czy można podszyć się pod nadawcę wiadomości SMS?	86
Na czym polega vishing?	86
Do czego można wykorzystać narzędzie Burp Suite?	86
Na czym polega credential stuffing?	86
Jak wygląda atak SIMSWAP?	87
Jakie znasz metody socjotechniki?	88
Na czym polega rekonesans i dlaczego jest ważny dla pentestera?	88
Po co firmowe laptopy są szyfrowane?	88
Na czym polega google hacking/google dorking?	89
Jakie popularne rodzaje cyberataków można wymienić?	89
Jak zapobiegać atakom typu brute force?	89
Czym różni się responsible disclosure od full disclosure?	90
Na czym polega atak clickjacking i jak się przed nim obronić?	90

Czym jest przechwytywanie sesji?	91
W jakim celu pentesterzy korzystają z serwerów proxy?	93
Czym jest Cyber Threat Intelligence (CTI)?	93
Na czym polega podatność SSRF?	93
W jaki sposób atak DoS na stronę firmową może zagrozić organizacji?	94
Czym jest OWASP Top 10?	94
Jakim narzędziem modyfikujesz ruch HTTP?	94
Czy CSS można wykorzystać do ataków?	95
Jakie projekty OWASP inne niż Top 10 można wymienić?	95
Do czego można wykorzystać portal Shodan?	96
Jak chronić się przed atakami phishingowymi?	96
Bibliografia	99

Kryptografia

Jakie informacje znajdują się w certyfikacie SSL?

Certyfikat SSL jest małym plikiem danych, który cyfrowo wiąże klucz kryptograficzny i służy do poświadczenia wiarygodności domeny oraz jej właściciela. Umożliwia dzięki temu ustanowienie bezpiecznego połączenia między przeglądarką a serwerem internetowym.

Certyfikat **SSL** zawiera dane strony, dla której został wydany:

- nazwa domeny,
- okres ważności certyfikatu,
- szczegóły dotyczące urzędu certyfikacji (CA),
- klucz publiczny i wersja SSL/TLS,
- algorytm klucza publicznego,
- algorytm podpisu certyfikatu.

MD5 czy SHA-256 — co jest lepsze i dlaczego?

SHA-2 (ang. *Secure Hash Algorithm*) — zestaw kryptograficznych funkcji skrótu (SHA-224, SHA-256, SHA-384, SHA-512), zaprojektowany przez National Security Agency (NSA) i opublikowany w 2001 roku przez National Institute of Standards and Technology (NIST) jako federalny standard przetwarzania informacji rządu Stanów Zjednoczonych. SHA-1, SHA-256, SHA-384 i SHA-512 to iteracyjne, jednokierunkowe funkcje skrótu, które mogą przetwarzać komunikat o maksymalnej długości od 2^{64} do 2^{128} bitów w celu uzyskania od 160- do 512-bitowej skróconej reprezentacji, zwanej skrótem wiadomości.

MD5 (ang. *Message Digest*) to wszechobecny algorytm haszujący, który został opracowany przez Rona Rivesta i jest obecnie wykorzystywany w wielu aplikacjach internetowych. Algorytm MD5 przyjmuje na wejściu komunikat o dowolnej długości i generuje jako wyjście

128-bitowy „odcisk palca” lub „skrót wiadomości” komunikatu wejściowego. Skrót MD5 jest zwykle wyrażany jako 32-cyfrowa liczba szesnastkowa i uważa się, że jest uszkodzony kryptograficznie i może mieć kolizje. Przez kolizję rozumiemy fakt, że różne komunikaty wejściowe mogą mieć taką samą funkcję skrótu.

Podobnie jak MD5, SHA jest również szeroko stosowany w aplikacjach, takich jak SSH, SSL, S-MIME (ang. *Secure/Multipurpose Mail Extension*) i IPsec.

Algorytm SHA jest nieco wolniejszy niż MD5, ale większa długość skrótu sprawia, że jest on bardziej zabezpieczony przed atakami inwersyjnymi i kolizją siłową.

Jakie znasz metody szyfrowania?

Wyróżnia się dwie metody szyfrowania danych: symetryczną oraz asymetryczną.

Szyfrowanie symetryczne — szyfrowanie, w którym klucz szyfrowania danych jest taki sam jak klucz do ich deszyfrowania. Odbiorca i nadawca muszą przed przekazaniem poufnych zaszyfrowanych informacji ustalić, jak będzie wyglądać tajny klucz oraz jakim bezpiecznym kanałem go sobie dostarczą. Metodą symetryczną szyfrowania jest m.in. kod Cezara, AES, One-Time i 3DES.

Szyfrowanie asymetryczne — szyfrowanie z użyciem klucza jawnego/publicznego i prywatnego. Klucz do szyfrowania jest inny od klucza do deszyfrowania. Klucz publiczny jest powszechnie znany. Każdy jego posiadacz może za jego pomocą zaszyfrować dowolne dane. Natomiast jedynie posiadacz klucza prywatnego może odszyfrować otrzymane szyfrogramy. Analogicznie: posiadacz klucza prywatnego może używać go do szyfrowania danych, pozwalając w ten sposób każdemu posiadaczowi odpowiadającego mu klucza publicznego odszyfrować je. Metodą asymetryczną szyfrowania jest m.in. RSA.

Kiedy mamy do czynienia z kolizją w kontekście kryptografii?

Ze względu na to, że liczba wyników funkcji skrótu jest skończona, może się okazać, że dla dwóch zupełnie różnych wartości wejściowych otrzymamy taką samą wartość skrótu. Taką sytuację nazywamy **kolizją**.

Kiedy stosuje się szyfr blokowy, a kiedy szyfr strumieniowy?

Szyfr blokowy i **szyfr strumieniowy** to metody używane do konwersji zwykłego tekstu bezpośrednio na tekst szyfru. Należą do rodziny symetrycznych szyfrów kluczy.

Główna różnica między szyfrem blokowym a szyfrem strumieniowym polega na tym, że ten pierwszy szyfruje i odszyfrowuje blok tekstu naraz. Z kolei szyfr strumieniowy szyfruje i odszyfrowuje tekst, przyjmując jeden bajt tekstu naraz.

Jakiej minimalnej długości powinno być hasło użytkownika?

Hasła powinny się składać z co najmniej ośmiu znaków oraz być złożone z małych i wielkich liter, cyfr lub znaków specjalnych. Należy oczywiście pamiętać, że jest to minimalna polityka haseł. Im dłuższe hasło, tym lepsze. Warto też zwrócić uwagę na czas, po jakim należy zmieniać hasła. Obecnie trendem jest ustanawianie dłuższych haseł (przynajmniej dwunastoznakowych) i okresu zmiany przynajmniej raz na 3 – 6 miesięcy.

Jaka jest różnica pomiędzy haszowaniem a szyfrowaniem?

Haszowanie to wyliczanie przy użyciu funkcji skrótu (algorytmu takiego jak na przykład MD5 czy SHA) unikalnego ciągu znaków o stałej długości dla dowolnego tekstu. Istotną cechą haszowania jest fakt, że jest to proces nieodwracalny.

Szyfrowanie to proces zamiany tekstu jawnego, zrozumiałego dla człowieka (ang. *cleartext*, *plaintext*), w szyfrogram (ang. *cryptogram*, *ciphertext*), czyli postać otrzymaną za pomocą serii przekształceń i podstawień, której nie da się odczytać ani odszyfrować bez znajomości klucza szyfrującego.

Po co stosujemy funkcje skrótu?

Funkcja skrótu (funkcja mieszająca lub funkcja haszująca) to funkcja przyporządkowująca dowolnie dużej liczbie krótką wartość o stałym rozmiarze, tzw. skrót nieodwracalny.

W informatyce funkcje skrótu pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych. Sygnatury mogą chronić przed przypadkowymi lub celowo wprowadzonymi modyfikacjami danych (sumy kontrolne), a także mają zastosowanie przy optymalizacji dostępu do struktur danych w programach komputerowych (tablice mieszające).

Co zapewnia kod HMAC?

HMAC (ang. *Keyed-Hash Message Authentication Code*, *Hash-based Message Authentication Code*) — kod **MAC** z włączonym kluczem tajnym, zapewniający zarówno ochronę integralności, jak i autentyczności danych.

Czy jest jakaś różnica pomiędzy SSL a TLS?

Najważniejszą różnicą pomiędzy SSL a TLS jest to, że **TLS** jest bezpieczniejszy. Wynika to z faktu, że TLS jest po prostu wyższą wersją **SSL**, z której to TLS wyewoluował. W istocie TLS 1.0 to SSL 3.1.

Zmiana nazewnictwa wynika z tego, że za stworzeniem SSL w 1994 roku stoi Netscape, który nie miał wkładu w wersję TLS z 1999 roku. Autorzy chcieli więc odciąć się od skojarzeń z Netscape.

Obecnie zamawiając czy instalując certyfikat SSL, tak naprawdę mamy do czynienia z certyfikatem TLS. Nazwa „certyfikaty SSL” pozostała w użyciu, ponieważ była już rozpowszechniona i szeroko stosowana.

Jaka jest przewaga kryptografii krzywych eliptycznych nad RSA?

Kryptografia krzywych eliptycznych (ang. *Elliptic Curve Cryptography*, ECC) wykorzystuje matematyczne właściwości krzywych eliptycznych do tworzenia systemów kryptograficznych z kluczem publicznym. Mniejsze rozmiary kluczy ECDSA (ang. *Elliptic Curve Digital Signature Algorithm*) oznaczają, że można osiągnąć silniejsze szyfrowanie przy mniejszej mocy obliczeniowej i przepustowości sieci niż w przypadku RSA. Jest to szczególnie korzystne w kontekście urządzeń mobilnych i internetu rzeczy (IoT) o niskiej mocy, które stają się coraz bardziej wszechobecne.

Do czego można użyć klucza publicznego?

Klucz publiczny używany w szyfrowaniu asymetrycznym (z użyciem pary kluczy publicznego i prywatnego) służy do szyfrowania informacji. Klucz publiczny jest powszechnie dostępny, jednak zaszyfrowane nim informacje może odczytać jedynie posiadacz **klucza prywatnego**. Możemy go wykorzystać do bezpiecznej komunikacji i do bezpiecznego połączenia z serwerem, na przykład przy użyciu SSH.

Jak zdefiniować salting i do czego jest on używany?

Salting to proces dodawania unikalnych losowych ciągów znaków do haseł w bazie danych lub każdego hasła przed zaszyfrowaniem hasła. Ma to na celu zmianę skrótu i zwiększenie bezpieczeństwa haseł. Ciąg znaków dodawany do hasła nazywa się solą. Sól można dodać przed lub za hasłem.

Sól nie jest upubliczniana i jest znana tylko lokalnie.

Do czego służą sól i pieprz w kontekście haszowania haseł?

Sól (ang. *salt*) — dane losowe dodawane do hasła podczas obliczania funkcji skrótu przechowywanej w systemach informatycznych. Celem soli jest ochrona systemowej bazy haseł przed atakami słownikowymi. Jako że sól jest przechowywana jawnie, nie ma ona znaczenia w przypadku ataków brute force.

Pieprz (ang. *pepper*) to statyczna, tajna wartość przechowywana oddzielnie od bazy danych (zawierającej hasze). Zwykle kodowana na twardo w kodzie źródłowym aplikacji. Chroni hasła przed atakami typu brute force.

Co oznacza utajnianie z wyprzedzeniem?

Utajnianie z wyprzedzeniem (ang. *Perfect Forward Secrecy*, PFS; zwane także *forward secrecy*, FS) odnosi się do systemu szyfrowania, który często i automatycznie zmienia klucze używane do szyfrowania oraz deszyfrowania informacji. Ten ciągły proces zapewnia, że nawet jeśli najnowszy klucz zostanie skompromitowany, ujawniona zostanie jedynie minimalna ilość poufnych danych.

Czym różni się zaufany certyfikat SSL od niezaufanego? Po co nam zaufane główne urzędy certyfikacji?

Podstawowe różnice między tymi certyfikatami to:

- **weryfikacja praw własności domeny** — ma ona miejsce dla certyfikatów komercyjnych, co zwiększa bezpieczeństwo usługi;
- **gwarancja** — jest to kwota pieniężna, jaką wypłaca jednostka certyfikująca w sytuacji, kiedy dojdzie do złamania klucza certyfikatu;
- **dotatkowa weryfikacja** — w przypadku certyfikatów OV i EV ma miejsce dodatkowa weryfikacja w postaci przesłania odpowiednich dokumentów do jednostki certyfikującej przed wystawieniem SSL, co zwiększa wiarygodność;
- **cena**;
- **czas** — certyfikaty komercyjne wystawiane są najczęściej na rok, po tym okresie należy ponownie aktywować usługę.

Urząd certyfikacji (ang. *Certificate Authority, CA*) — podmiot, który wystawia certyfikaty cyfrowe. Certyfikat potwierdza własność klucza publicznego poprzez wskazanie podmiotu certyfikatu. Pozwala to innym powołującym się stronom polegać na podpisach lub zapewnieniach złożonych przez klucz prywatny odpowiadający kluczowi publicznemu. W tym modelu relacji zaufania CA jest zaufaną stroną trzecią.

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 

CYBERSECURITY

w pytaniach i odpowiedziach

Co o cyberbezpieczeństwie każdy wiedzieć powinien

W świecie, w którym większość naszych mniej lub bardziej wrażliwych danych przechowywana jest w sieci, cyberbezpieczeństwo powinno być tematem numer jeden. Niestety, na ogół nie jest, bo... Po prostu nie chce się nam myśleć o zastosowaniu odpowiednich zabezpieczeń. Stają się one dla nas kluczowe dopiero, kiedy ktoś się cyberwłamie i realnie skradnie coś, co było dla nas istotne: hasło do poczty e-mail, pieniądze z konta w banku, zdjęcia, które wolelibyśmy zachować dla siebie, itd. Tyle że wtedy jest już za późno.

Ta książka powstała po to, by jej czytelnik zdążył wyprzedzić zagrożenie. Stanowi wprowadzenie do zagadnienia cyberbezpieczeństwa. Podzielona na kilka kluczowych części (systemy operacyjne, sieci komputerowe, aplikacje webowe, kryptografia, wreszcie cyberbezpieczeństwo jako takie), pozwala zapoznać się z najważniejszymi zagrożeniami i ze sposobami zabezpieczeń. Przybliża terminologię związaną z tematem i stanowi świetny punkt wyjścia do dalszego zgłębiania jego wybranych aspektów.

Cyberniebezpieczeństwo czyha. Czy jesteś na nie przygotowany?

		KOD KORZYŚCI Sięgnij po więcej! ▶	
	helion.pl	ISBN 978-83-283-9924-2	
	HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	 9 788328 399242	
Cena: 39,90 zł			