

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! Załoguj 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
Następowanie trojana	74
Infekowanie maszyny wirtualnej z systemem Windows	76
Kontrolowanie maszyny wirtualnej z systemem Windows za pomocą Meterpretera	79
Przeglądanie i przysyłanie 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	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. Chroni 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