

**Podstawy systemu Linux dla hakerów : pierwsze kroki z sieciami,  
skryptami i zabezpieczeniami w systemie Kali / Bryson Payne. –  
Wydanie I. – Warszawa, 2020**

Spis treści

|                                                                           |            |
|---------------------------------------------------------------------------|------------|
| <b>PODZIĘKOWANIA</b>                                                      | <b>xix</b> |
| <b>WPROWADZENIE</b>                                                       | <b>xxi</b> |
| Zawartość książki                                                         | xxii       |
| Co to jest „hakerstwo etyczne”?                                           | xxiii      |
| Testowanie penetracyjne                                                   | xxiii      |
| Działania wojskowe i wywiadowcze                                          | xxiv       |
| Dlaczego hakerzy używają Linuksa                                          | xxiv       |
| Linux jest systemem typu „open source”                                    | xxiv       |
| Linux jest systemem transparentnym                                        | xxiv       |
| Linux oferuje granularną kontrolę                                         | xxv        |
| Większość narzędzi hakerskich jest napisana dla systemu Linux             | xxv        |
| Przyszłość należy do systemów Linux i Unix                                | xxv        |
| Pobieranie oprogramowania Kali Linux                                      | xxv        |
| Maszyny wirtualne                                                         | xxvii      |
| Instalowanie maszyny wirtualnej VirtualBox                                | xxvii      |
| Konfigurowanie maszyny wirtualnej                                         | xxix       |
| Instalowanie systemu Kali w maszynie wirtualnej                           | xxxii      |
| Konfigurowanie systemu Kali                                               | xxxiii     |
| <b>1</b>                                                                  |            |
| <b>PODSTAWY - PIERWSZE KROKI</b>                                          | <b>1</b>   |
| Podstawowe terminy i pojęcia                                              | 1          |
| Krótki przegląd systemu Kali                                              | 3          |
| Terminal                                                                  | 4          |
| System plików w Linuksie                                                  | 4          |
| Podstawowe polecenia w systemie Linux                                     | 5          |
| Ustalanie obecnego miejsca za pomocą polecenia pwd                        | 6          |
| Sprawdzanie swojej nazwy użytkownika za pomocą polecenia whoami           | 6          |
| Poruszanie się po systemie plików w Linuksie                              | 7          |
| Uzyskiwanie pomocy                                                        | 9          |
| Odwoływanie się do stron podręczników za pomocą polecenia man             | 9          |
| Odnajdywanie obiektów                                                     | 10         |
| Wyszukiwanie za pomocą polecenia locate                                   | 10         |
| Odnajdywanie binariów za pomocą polecenia whereis                         | 11         |
| Znajdowanie binariów dostępnych na ścieżce PATH za pomocą polecenia which | 11         |
| Bardziej zaawansowane wyszukiwanie za pomocą polecenia find               | 11         |
| Filtrowanie za pomocą polecenia grep                                      | 13         |
| Modyfikowanie plików i katalogów                                          | 14         |

|                     |    |
|---------------------|----|
| Tworzenie pliku     | 14 |
| Tworzenie katalogu  | 16 |
| Kopiowanie pliku    | 16 |
| Zmianie nazwy pliku | 16 |
| Usuwanie pliku      | 17 |
| Usuwanie katalogu   | 17 |
| Poeksperymentujmy!  | 18 |
| Ćwiczenia           | 18 |

## 2

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>OPERACJE NA TEKSTACH</b>                                  | <b>19</b> |
| Wyświetlanie plików                                          | 20        |
| Wyświetlanie początku za pomocą polecenia head               | 20        |
| Wyświetlanie końca za pomocą polecenia tail                  | 21        |
| Numerowanie linii                                            | 22        |
| Filtrowanie tekstu za pomocą polecenia grep                  | 22        |
| Zadanie dla hakerów: użycie poleceń grep, nl, tail i head    | 23        |
| Wyszukiwanie i zastępowanie za pomocą polecenia sed          | 24        |
| Wyświetlanie zawartości plików za pomocą poleceń more i less | 25        |
| Sterowanie wyświetlaniem za pomocą polecenia more            | 25        |
| Wyświetlanie i filtrowanie za pomocą polecenia less          | 26        |
| Podsumowanie                                                 | 27        |
| Ćwiczenia                                                    | 27        |

## 3

|                                                              |           |
|--------------------------------------------------------------|-----------|
| <b>ANALIZOWANIE SIECI I ZARZĄDZANIE NIMI</b>                 | <b>29</b> |
| Analizowanie sieci za pomocą narzędzia ifconfig              | 29        |
| Sprawdzanie urządzeń sieciowych za pomocą narzędzia iwconfig | 30        |
| Zmianie swoich danych sieciowych                             | 31        |
| Zmianie swojego adresu IP                                    | 31        |
| Zmianie swojej maski sieci i swojego adresu rozgłoszeniowego | 32        |
| Zmianie swojego adresu MAC                                   | 32        |
| Przypisywanie nowego adresu IP z serwera DHCP                | 32        |
| Korzystanie z usługi DNS                                     | 33        |
| Badanie usługi DNS za pomocą polecenia dig                   | 33        |
| Zmianie swojego serwera DNS                                  | 35        |
| Odwzorowywanie własnych adresów IP                           | 36        |
| Podsumowanie                                                 | 37        |
| Ćwiczenia                                                    | 37        |

## 4

|                                                |           |
|------------------------------------------------|-----------|
| <b>DODAWANIE I USUWANIE OPROGRAMOWANIA</b>     | <b>39</b> |
| Obsługa oprogramowania za pomocą narzędzia apt | 40        |
| Wyszukiwanie pakietu                           | 40        |
| Dodawanie oprogramowania                       | 40        |
| Usuwanie oprogramowania                        | 41        |
| Aktualizowanie pakietów                        | 42        |
| Uaktualnianie pakietów                         | 43        |

|                                                     |    |
|-----------------------------------------------------|----|
| Dodawanie repozytoriów do pliku sources.list        | 43 |
| Używanie instalatora graficznego                    | 45 |
| Instalowanie oprogramowania za pomocą narzędzia git | 47 |
| Podsumowanie                                        | 48 |
| Ćwiczenia                                           | 48 |

## 5

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>KONTROLOWANIE UPRAWNIEŃ DO PLIKÓW I KATALOGÓW</b>                    | <b>49</b> |
| Różne rodzaje użytkowników                                              | 50        |
| Nadawanie uprawnień                                                     | 50        |
| Przypisywanie praw własności indywidualnemu użytkownikowi               | 51        |
| Przypisywanie praw własności grupie                                     | 51        |
| Sprawdzanie uprawnień                                                   | 51        |
| Zmienianie uprawnień                                                    | 53        |
| Zmienianie uprawnień z użyciem notacji dziesiętnej                      | 53        |
| Zmienianie uprawnień z użyciem składni UGO                              | 55        |
| Nadawanie użytkownikowi root uprawnień do uruchamiania nowego narzędzia | 56        |
| Ustawianie bardziej bezpiecznych ustawień domyślnych z użyciem masek    | 57        |
| Uprawnienia specjalne                                                   | 58        |
| Nadawanie tymczasowych uprawnień właściciela za pomocą ustawienia SUID  | 58        |
| Nadawanie uprawnień grupy właściciela za pomocą ustawienia SGID         | 58        |
| Przestarzały „sticky bit”                                               | 59        |
| Uprawnienia specjalne, eskalacja uprawnień i hakerzy                    | 59        |
| Podsumowanie                                                            | 60        |
| Ćwiczenia                                                               | 61        |

## 6

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| <b>ZARZĄDZANIE PROCESAMI</b>                                             | <b>63</b> |
| Wyświetlanie procesów                                                    | 64        |
| Filtrowanie z użyciem nazwy procesu                                      | 65        |
| Znajdowanie najbardziej zasobochłonnych procesów za pomocą polecenia top | 66        |
| Zarządzanie procesami                                                    | 67        |
| Zmienianie priorytetu procesu za pomocą polecenia nice                   | 67        |
| Likwidowanie procesów                                                    | 69        |
| Uruchamianie procesów w tle                                              | 70        |
| Przenoszenie procesu do planu pierwszego                                 | 71        |
| Planowanie procesów                                                      | 71        |
| Podsumowanie                                                             | 72        |
| Ćwiczenia                                                                | 72        |

## 7

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>ZARZĄDZANIE ZMIENNYMI ŚRODOWISKOWYMI UŻYTKOWNIKA</b> | <b>73</b> |
| Wyświetlanie i modyfikowanie zmiennych środowiskowych   | 74        |
| Wyświetlanie wszystkich zmiennych środowiskowych        | 74        |

|                                                    |    |
|----------------------------------------------------|----|
| Filtrowanie pod kątem określonych zmiennych        | 75 |
| Zmienianie wartości zmiennych dla sesji            | 75 |
| Utrwalanie zmian wartości zmiennej                 | 76 |
| Zmienianie znaku zachęty powłoki                   | 76 |
| Modyfikowanie zmiennej PATH                        | 78 |
| Dodawanie katalogów do zmiennej PATH               | 78 |
| Jak nie dodawać do zmiennej PATH                   | 79 |
| Tworzenie zmiennej zdefiniowanej przez użytkownika | 79 |
| Podsumowanie                                       | 80 |
| Ćwiczenia                                          | 80 |

## 8

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| <b>SKRYPTY POWŁOKI BASH</b>                                                                | <b>81</b> |
| Błyskawiczny kurs powłoki bash                                                             | 82        |
| Nasz pierwszy skrypt „Hello, Hackers-Arise!”                                               | 82        |
| Ustawianie uprawnień do wykonywania                                                        | 83        |
| Uruchamianie skryptu HelloHackersArise                                                     | 84        |
| Zwiększanie funkcjonalności za pomocą zmiennych i informacji podawanych przez użytkowników | 84        |
| Pierwszy skrypt hakerski: skanowanie w celu wyszukania otwartych portów                    | 86        |
| Nasze zadanie                                                                              | 87        |
| Prosty skaner                                                                              | 87        |
| Udoskonalanie skanera MySQL                                                                | 88        |
| Często używane polecenia powłoki bash                                                      | 91        |
| Podsumowanie                                                                               | 92        |
| Ćwiczenia                                                                                  | 92        |

## 9

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <b>KOMPRESJA I ARCHIWIZACJA</b>                                    | <b>93</b> |
| Na czym polega kompresja?                                          | 93        |
| Grupowanie plików w archiwum                                       | 94        |
| Kompresowanie plików                                               | 96        |
| Kompresowanie za pomocą narzędzia gzip                             | 96        |
| Kompresowanie za pomocą narzędzia bzip2                            | 97        |
| Kompresowanie za pomocą narzędzia compress                         | 97        |
| Tworzenie fizycznych kopii „bit po bicie” urządzeń pamięci masowej | 98        |
| Podsumowanie                                                       | 99        |
| Ćwiczenia                                                          | 99        |

## 10

|                                                                   |            |
|-------------------------------------------------------------------|------------|
| <b>ZARZĄDZANIE SYSTEMEM PLIKÓW I URZĄDZENIAMI PAMIĘCI MASOWEJ</b> | <b>101</b> |
| Katalog/dev urządzeń                                              | 102        |
| W jaki sposób Linux przedstawia urządzenia pamięci masowej        | 103        |
| Partycje dysków                                                   | 103        |
| Urządzenia znakowe i blokowe                                      | 105        |
| Wyświetlanie informacji o urządzeniach blokowych za pomocą        |            |

|                                                 |     |
|-------------------------------------------------|-----|
| polecenia Isblk                                 | 105 |
| Montowanie i odmontowywanie                     | 106 |
| Samodzielne montowanie urządzeń pamięci masowej | 106 |
| Odmontowywanie za pomocą polecenia umount       | 107 |
| Monitorowanie systemów plików                   | 107 |
| Uzyskiwanie informacji o zamontowanych dyskach  | 107 |
| Sprawdzanie pod kątem błędów                    | 108 |
| Podsumowanie                                    | 109 |
| Ćwiczenia                                       | 110 |

## 11

|                                                                       |            |
|-----------------------------------------------------------------------|------------|
| <b>SYSTEM REJESTROWANIA W DZIENNIKACH</b>                             | <b>111</b> |
| Proces demon rsyslog                                                  | 112        |
| Plik konfiguracyjny rsyslog                                           | 112        |
| Reguły narzędzia rsyslog                                              | 113        |
| Automatyczne usuwanie plików dzienników za pomocą narzędzia logrotate | 115        |
| Niewidzialność                                                        | 117        |
| Usuwanie śladów                                                       | 117        |
| Wyłączanie rejestrowania w dziennikach                                | 119        |
| Podsumowanie                                                          | 119        |
| Ćwiczenia                                                             | 119        |

## 12

|                                                                         |            |
|-------------------------------------------------------------------------|------------|
| <b>KORZYSTANIE Z USŁUG I ICH WYKORZYSTYWANIE</b>                        | <b>121</b> |
| Uruchamianie, zatrzymywanie i restartowanie usług                       | 122        |
| Tworzenie internetowego serwera HTTP za pomocą usługi Apache Web Server | 122        |
| Pierwsze kroki z usługą Apache                                          | 123        |
| Edytowanie pliku index.html                                             | 124        |
| Dodawanie treści w formacie HTML                                        | 124        |
| Co uzyskaliśmy                                                          | 125        |
| OpenSSH i Raspberry Spy Pi                                              | 125        |
| Przygotowanie urządzenia Raspberry Pi                                   | 126        |
| Konstruowanie systemu Raspberry Spy Pi                                  | 126        |
| Konfigurowanie kamery                                                   | 127        |
| Rozpoczynanie szpiegowania                                              | 129        |
| Wydobywanie informacji z baz danych MySQL                               | 130        |
| Uruchamianie bazy danych MySQL                                          | 130        |
| Komunikowanie się z bazą danych MySQL                                   | 131        |
| Ustawianie hasła do bazy danych MySQL                                   | 132        |
| Uzyskiwanie dostępu do odległej bazy danych                             | 133        |
| Łączenie się z bazą danych                                              | 133        |
| Tabele bazy danych                                                      | 134        |
| Badanie danych                                                          | 135        |
| PostgreSQL i środowisko Metasploit                                      | 135        |
| Podsumowanie                                                            | 138        |
| Ćwiczenia                                                               | 138        |

## **13**

### **ZAPEWNIANIE SOBIE BEZPIECZEŃSTWA I ANONIMOWOŚCI 139**

|                                                            |     |
|------------------------------------------------------------|-----|
| W jaki sposób Internet nas zdradza                         | 140 |
| System „The Onion Router”                                  | 141 |
| Jak działa sieć Tor                                        | 141 |
| Kwestie bezpieczeństwa                                     | 142 |
| Serwery proxy                                              | 143 |
| Określanie serwerów proxy za pomocą pliku konfiguracyjnego | 144 |
| Kilka innych interesujących opcji                          | 146 |
| Kwestie bezpieczeństwa                                     | 148 |
| Wirtualne sieci prywatne                                   | 149 |
| Szyfrowana poczta elektroniczna                            | 150 |
| Podsumowanie                                               | 151 |
| Ćwiczenia                                                  | 151 |

## **14**

### **OMÓWIENIE SIECI BEZPRZEWODOWYCH I ICH BADANIE 153**

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Sieci Wi-Fi                                                      | 154 |
| Podstawowe polecenia dla sieci bezprzewodowych                   | 155 |
| Rozpoznawanie sieci Wi-Fi za pomocą pakietu narzędzi aircrack-ng | 158 |
| Wykrywanie urządzeń Bluetooth i podłączanie się do nich          | 160 |
| Jak działa Bluetooth                                             | 160 |
| Skanowanie urządzeń Bluetooth i rekonesans                       | 161 |
| Podsumowanie                                                     | 164 |
| Ćwiczenia                                                        | 165 |

## **15**

### **ZARZĄDZANIE JĄDREM SYSTEMU LINUX I ŁADOWALNYMI MODUŁAMI JĄDRA 167**

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| Co to jest „moduł jądra”?                                          | 168 |
| Sprawdzanie wersji jądra systemu                                   | 169 |
| Dostrajanie jądra za pomocą polecenia sysctl                       | 169 |
| Zarządzanie modułami jądra                                         | 171 |
| Uzyskiwanie dokładniejszych informacji za pomocą polecenia modinfo | 172 |
| Dodawanie i usuwanie modułów za pomocą polecenia modprobe          | 173 |
| Wstawianie i usuwanie modułów jądra                                | 173 |
| Podsumowanie                                                       | 174 |
| Ćwiczenia                                                          | 174 |

## **16**

### **AUTOMATYZOWANIE ZADAŃ ZA POMOCĄ FUNKCJI PLANOWANIA ZLECEŃ 175**

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Planowanie zdarzenia lub zlecenia do automatycznego uruchamiania     | 176 |
| Planowanie zadania sporządzania kopii zapasowej                      | 178 |
| Planowanie uruchamiania skryptu MySQLscanner z użyciem pliku crontab | 179 |
| Skróty crontab                                                       | 180 |

|                                                                         |            |
|-------------------------------------------------------------------------|------------|
| Używanie skryptów rc do uruchamiania zleceń wraz z systemem             | 181        |
| Poziomy uruchamiania w systemie Linux                                   | 181        |
| Dodawanie usług do skryptu rc.d                                         | 181        |
| Dodawanie usług startowych za pomocą graficznego interfejsu użytkownika | 182        |
| Podsumowanie                                                            | 183        |
| Ćwiczenia                                                               | 183        |
| <br><b>17</b>                                                           |            |
| <b>PODSTAWY SKRYPTÓW PYTHON DLA HAKERÓW</b>                             | <b>185</b> |
| Dodawanie modułów Python                                                | 186        |
| Korzystanie z menedżera pakietów pip                                    | 187        |
| Instalowanie modułów podmiotów trzecich                                 | 187        |
| Wprowadzenie do pisania skryptów w języku Python                        | 188        |
| Zmienne                                                                 | 189        |
| Komentarze                                                              | 192        |
| Funkcje                                                                 | 193        |
| Listy                                                                   | 193        |
| Moduły                                                                  | 194        |
| Programowanie obiektowe                                                 | 194        |
| Python a komunikacja sieciowa                                           | 196        |
| Tworzenie klienta TCP                                                   | 196        |
| Tworzenie nasłuchu TCP                                                  | 197        |
| Słowniki, instrukcje sterujące i pętle                                  | 199        |
| Słowniki                                                                | 199        |
| Instrukcje sterujące                                                    | 199        |
| Pętle                                                                   | 200        |
| Udoskonalanie naszych hakerskich skryptów                               | 201        |
| Wyjątki i łamacze haseł                                                 | 203        |
| Podsumowanie                                                            | 205        |
| Ćwiczenia                                                               | 205        |
| <br><b>SKOROWIDZ</b>                                                    | <b>207</b> |