

Spis treści

Przedmowa	11
-----------------	----

CZĘŚĆ I. Podstawy 15

1. Wprowadzenie do wiersza poleceń 17

Definicja wiersza poleceń	17
---------------------------	----

Dlaczego bash?	18
----------------	----

Przykłady wykonywane w wierszu poleceń	18
--	----

Uruchamianie Linuksa i basha w systemie Windows	18
---	----

Git Bash	18
----------	----

Cygwin	19
--------	----

Podsystem Windows dla systemu Linux	19
-------------------------------------	----

Wiersz polecenia systemu Windows i PowerShell	20
---	----

Podstawy wiersza poleceń	20
--------------------------	----

Polecenia, argumenty, polecenia wbudowane i słowa kluczowe	21
--	----

Standardowy strumień wejścia, wyjścia i błędów	22
--	----

Przekierowania i potoki	22
-------------------------	----

Uruchamianie poleceń w tle	23
----------------------------	----

Od wiersza poleceń do skryptu	24
-------------------------------	----

Podsumowanie	24
--------------	----

Ćwiczenia	25
-----------	----

2. Podstawy basha 27

Wyniki	27
--------	----

Zmienne	28
---------	----

Parametry pozycyjne	28
---------------------	----

Dane wejściowe	29
----------------	----

Instrukcje warunkowe	29
----------------------	----

Pętle	33
-------	----

Funkcje	34
Argumenty funkcji	35
Zwracanie wartości	35
Dopasowywanie wzorców w bashu	36
Pisanie pierwszego skryptu — wykrywanie typu systemu operacyjnego	37
Podsumowanie	38
Ćwiczenia	39
3. Wprowadzenie do wyrażeń regularnych	41
Wykorzystywane polecenia	41
grep	41
grep i egrep	42
Metaznaki wyrażeń regularnych	43
Metaznak „.”	43
Metaznak „?”	43
Metaznak „*”	43
Metaznak „+”	44
Grupowanie	44
Nawiasy kwadratowe i klasy znakowe	44
Odwołania wsteczne	46
Kwantyfikatory	47
Kotwice i granice słów	47
Podsumowanie	48
Ćwiczenia	48
4. Zasady działań defensywnych i ofensywnych	49
Cyberbezpieczeństwo	49
Poufność	49
Integralność	50
Dostępność	50
Niezaprzeczalność	50
Uwierzytelnianie	50
Cykl życia ataku	51
Rekonesans	51
Wstępna eksploatacja	51
Ustanowienie punktu zaczepienia	52
Eskalacja uprawnień	52
Rekonesans wewnętrzny	52
Ruch boczny	53
Utrzymanie obecności	53
Zakończenie misji	53
Podsumowanie	53

CZĘŚĆ II. Defensywne działania związane z bezpieczeństwem w bashu **55**

5. Zbieranie danych	57
Wykorzystywane polecenia	58
cut	58
file	59
head	59
reg	60
wevtutil	60
Zbieranie informacji systemowych	61
Zdalne wykonywanie poleceń za pomocą SSH	61
Zbieranie plików dziennika w Linuksie	62
Zbieranie plików dzienników w systemie Windows	63
Zbieranie informacji systemowych	65
Zbieranie danych z rejestru systemu Windows	69
Przeszukiwanie systemu plików	69
Przeszukiwanie według nazwy pliku	69
Szukanie ukrytych plików	70
Wyszukiwanie według rozmiaru pliku	71
Wyszukiwanie według czasu	72
Szukanie określonej treści	72
Wyszukiwanie według typu pliku	73
Przeszukiwanie według wartości skrótu wiadomości	77
Transfer danych	79
Podsumowanie	79
Ćwiczenia	79
6. Przetwarzanie danych	81
Wykorzystywane polecenia	81
awk	81
join	82
sed	83
tail	84
tr	84
Przetwarzanie plików rozdzielanych	85
Iterowanie rozdzielanych danych	86
Przetwarzanie według pozycji znaku	87
Przetwarzanie plików XML	87
Przetwarzanie formatu JSON	89
Agregowanie danych	90
Podsumowanie	92
Ćwiczenia	92

7. Analiza danych	93
Wykorzystywane polecenia	93
sort	93
uniq	94
Omówienie dzienników dostępu na serwerze WWW	94
Sortowanie i porządkowanie danych	96
Liczba wystąpień w danych	96
Sumowanie liczb występujących w danych	100
Wyświetlanie danych na histogramie	101
Znajdowanie unikalnych danych	106
Szukanie anomalii w danych	108
Podsumowanie	110
Ćwiczenie	110
8. Monitorowanie dzienników w czasie rzeczywistym	113
Monitorowanie dzienników tekstowych	113
Wykrywanie włamań na podstawie wpisów w dziennikach	115
Monitorowanie dzienników systemu Windows	116
Generowanie histogramu w czasie rzeczywistym	117
Podsumowanie	121
Ćwiczenia	121
9. Narzędzie: monitor sieci	123
Wykorzystywane polecenia	123
crontab	123
schtasks	124
Krok 1. Tworzenie skanera portów	124
Krok 2. Porównanie z poprzednim wynikiem	126
Krok 3. Automatyzacja i powiadomienia	128
Planowanie zadania w Linuksie	130
Planowanie zadania w systemie Windows	131
Podsumowanie	131
Ćwiczenia	131
10. Narzędzie: monitorowanie systemu plików	133
Wykorzystywane polecenia	133
sdiff	133
Krok 1. Wyznaczanie początkowego stanu systemu plików	134
Krok 2. Wykrywanie zmian względem punktu odniesienia	135
Krok 3. Automatyzacja i powiadomienia	137
Podsumowanie	140
Ćwiczenia	140

11. Analiza złośliwego oprogramowania	143
Wykorzystywane polecenia	143
curl	143
vi	144
xxd	145
Inżynieria odwrotna	145
Przekształcenia między danymi heksadecymalnymi, dziesiętnymi, binarnymi i ASCII	146
Analizowanie za pomocą polecenia xxd	146
Wyodrębnianie ciągów tekstowych	148
Użycie narzędzia VirusTotal	149
Przeszukiwanie bazy danych według wartości skrótu	150
Skanowanie pliku	154
Skanowanie adresów URL, domen i adresów IP	154
Podsumowanie	155
Ćwiczenia	155
12. Formatowanie i raportowanie	157
Wykorzystywane polecenia	157
tput	157
Formatowanie i drukowanie danych w formacie HTML	158
Tworzenie pulpitu	161
Podsumowanie	166
Ćwiczenia	166
CZĘŚĆ III. Testy penetracyjne w bashu	167
13. Rekonesans	169
Wykorzystywane polecenia	169
ftp	169
Indeksowanie witryn WWW	170
Automatyczne pobieranie banera	171
Podsumowanie	175
Ćwiczenia	175
14. Obfuskacja skryptu	177
Wykorzystywane polecenia	177
base64	177
eval	178
Obfuskacja składni	178
Obfuskacja logiki	180

Szyfrowanie	182
Podstawy kryptografii	182
Szyfrowanie skryptu	183
Tworzenie wrappera	184
Tworzenie własnego algorytmu kryptograficznego	185
Podsumowanie	191
Ćwiczenia	191
15. Narzędzie: Fuzzing w wierszu poleceń	193
Implementacja	194
Podsumowanie	197
Ćwiczenia	197
16. Tworzenie punktu zaczepienia	199
Wykorzystywane polecenia	199
nc	199
Jednowierszowe tylne drzwi	200
Odwrotne połączenie SSH	200
Tylne drzwi w bashu	201
Własne narzędzie do dostępu zdalnego	202
Implementacja	203
Podsumowanie	206
Ćwiczenia	207
CZĘŚĆ IV. Administracja bezpieczeństwem w bashu	209
17. Użytkownicy, grupy i uprawnienia	211
Wykorzystywane polecenia	211
chmod	211
chown	212
getfacl	212
groupadd	212
setfacl	212
useradd	213
usermod	213
icacfs	213
net	214
Użytkownicy i grupy	214
Tworzenie użytkowników i grup w Linuksie	214
Tworzenie użytkowników i grup w systemie Windows	215

Uprawnienia do plików i listy kontroli dostępu	216
Uprawnienia do plików w Linuksie	216
Uprawnienia do plików w systemie Windows	218
Wprowadzanie masowych zmian	219
Podsumowanie	219
Ćwiczenia	219
18. Tworzenie wpisów w dziennikach	221
Wykorzystywane polecenia	221
eventcreate	221
logger	222
Tworzenie dzienników w systemie Windows	222
Tworzenie wpisów w dziennikach Linuksa	223
Podsumowanie	223
Ćwiczenia	224
19. Narzędzie: monitor dostępności systemu	225
Wykorzystywane polecenia	225
ping	225
Implementacja	226
Podsumowanie	228
Ćwiczenia	228
20. Narzędzie: ewidencja oprogramowania	229
Wykorzystywane polecenia	229
apt	230
dpkg	230
wmc	231
yum	231
Implementacja	232
Identyfikowanie innego oprogramowania	233
Podsumowanie	234
Ćwiczenia	234
21. Narzędzie: walidacja konfiguracji	235
Implementacja	235
Podsumowanie	239
Ćwiczenie	240

22. Narzędzie: inspekcja konta	241
Have I Been Pwned?	241
Sprawdzanie, czy hasło nie wyciekło	241
Sprawdzanie wycieku adresów e-mail	244
Masowe przetwarzanie adresów e-mail	246
Podsumowanie	247
Ćwiczenia	248
23. Konkluzje	249