

SŁOWO WSTĘPNE	11
PRZEDMOWA	15
Dlaczego należy ufać Mono?	16
Dla kogo jest ta książka?	16
Organizacja tej książki	17
Podziękowania	19
Ostatnia uwaga	19
1.	
BŁYSKAWICZNY KURS JĘZYKA C#	21
Wybór środowiska IDE	22
Prosty przykład	22
Wprowadzenie do klas i interfejsów	24
Tworzenie klasy	24
Tworzenie interfejsu	25
Tworzenie podklas klasy abstrakcyjnej i implementacja interfejsu	26
Powiązanie wszystkiego z metodą Main()	28
Uruchamianie metody Main()	30
Metody anonimowe	30
Przypisywanie delegata do metody	30
Aktualizacja klasy Firefighter	31
Tworzenie argumentów opcjonalnych	31
Aktualizacja metody Main()	32
Uruchomienie zaktualizowanej metody Main()	33
Integracja z bibliotekami natywnymi	34
Podsumowanie	35
2	
FUZZING. WYKORZYSTANIE XSS ORAZ INIEKCJI SQL	37
Konfigurowanie maszyny wirtualnej	38
Dodawanie sieci wirtualnej „tylko do hosta”	38
Tworzenie maszyny wirtualnej	39
Uruchamianie maszyny wirtualnej z obrazu ISO z systemem BadStore	39
Iniekcje SQL	41
Skrypty krzyżowe	43
Fuzzing żądań GET z wykorzystaniem fuzzera mutacyjnego	45
Preparowanie parametrów i testowanie luk	46
Budowanie żądań HTTP	47
Testowanie fuzzowanego kodu	48
Fuzzowanie żądań POST	49
Pisanie fuzzera żądania POST	50
Rozpoczyna się fuzzing	52
Fuzzowanie parametrów	54
Fuzzowanie danych w formacie JSON	56
Konfigurowanie wrażliwego urządzenia	56
Przechwytywanie wrażliwych żądań JSON	56

Tworzenie fuzzera JSON	57
Testowanie fuzzera JSON	62
Wykorzystywanie iniekcji SQL	63
Wykorzystywanie eksploita bazującego na instrukcji UNION ręcznie	64
Wykorzystywanie eksploita bazującego na instrukcji UNION programowo	66
Wykorzystywanie luk SQL typu Boolean-blind	70
Podsumowanie	79

3

FUZZOWANIE PUNKTÓW KOŃCOWYCH SOAP	81
Konfiguracja wrażliwych punktów końcowych	82
Parsowanie pliku WSDL	83
Tworzenie klasy dla dokumentu WSDL	84
Podstawowe metody parsowania	85
Klasy dla typu SOAP i parametrów	87
Tworzenie klasy SoapMessage definiującej przesyłane dane	90
Implementacja klasy reprezentującej części komunikatu	90
Definiowanie operacji portu za pomocą klasy SoapPortType	91
Implementacja klasy zawierającej operacje na porcie	93
Definiowanie protokołów używanych w powiązaniach SOAP	93
Kompilacja listy operacji węzłów potomnych	95
Znajdowanie usług SOAP w portach	96
Automatyczne fuzzowanie punktów końcowych SOAP pod kątem wrażliwości na iniekcje SQL	98
Fuzzowanie pojedynczych usług SOAP	99
Fuzzowanie portów SOAP HTTP POST	103
Fuzzowanie portu XML usługi SOAP	106
Uruchomienie fuzzera	110
Podsumowanie	111

4

PISANIE ŁADUNKÓW TYPU CONNECT-BACK, BIND I METASPLOIT	113
Tworzenie ładunku Connect-Back	114
Strumień sieci	114
Uruchomienie polecenia	116
Uruchomienie ładunku	117
Wiązanie ładunku	118
Odbieranie danych, uruchamianie poleceń i zwracanie wyników	119
Uruchamianie poleceń ze strumienia	120
Wykorzystanie protokołu UDP do ataku na sieć	121
Kod dla komputera docelowego	122
Kod napastnika	125
Uruchamianie ładunków typu Metasploit x86 i x86-64 za pomocą języka C#	128
Konfigurowanie frameworka Metasploit	128
Generowanie ładunków	130
Wykonywanie natywnych ładunków systemu Windows jako kodu niezarządzanego	131
Uruchamianie natywnych ładunków w systemie Linux	133

Podsumowanie	137
5	
AUTOMATYZACJA SKANERA NESSUS	139
REST i API systemu Nessus	140
Klasa NessusSession	141
Wykonywanie żądań HTTP	142
Wylogowanie i sprząatanie	144
Testowanie klasy NessusSession	145
Klasa NessusManager	146
Wykonywanie skanowania Nessus	148
Podsumowanie	150
6	
AUTOMATYZACJA N EXPOSE	153
Instalacja Nexpose	154
Aktywacja i testowanie	155
Żargon Nexpose	156
Klasa NexposeSession	157
Metoda ExecuteCommand()	158
Wylogowanie i zniszczenie sesji	161
Znajdowanie wersji interfejsu API	162
Korzystanie z Nexpose API	163
Klasa NexposeManager	163
Automatyzacja skanowania słabych punktów	165
Tworzenie lokalizacji z aktywami	165
Rozpoczynanie skanowania	166
Tworzenie raportu na temat lokalizacji w formacie PDF i usuwanie lokalizacji	167
Kompletowanie rozwiązania	168
Rozpoczęcie skanowania	169
Generowanie raportu i usuwanie lokalizacji	170
Uruchamianie automatyzacji	170
Podsumowanie	171
7	
AUTOMATYZACJA OPENVAS	173
Instalacja systemu OpenVAS	173
Budowanie klas	174
Klasa OpenVaSSession	175
Uwierzytelnianie na serwerze OpenVAS	176
Tworzenie metody do uruchamiania poleceń OpenVAS	177
Odczytywanie komunikatu z serwera	177
Konfiguracja strumienia TCP do wysyłania i odbierania poleceń	178
Walidacja certyfikatów i odświeżanie	179
Odczytywanie wersji OpenVAS	180
Klasa OpenVASManager	181
Pobieranie konfiguracji skanowania i tworzenie celów	182
Opakowanie automatyzacji	186
Uruchamianie automatyzacji	187
Podsumowanie	187

8

AUTOMATYZOWANIE PROGRAMU CUCKOO SANDBOX	189
Konfigurowanie Cuckoo Sandbox	190
Ręczne uruchamianie API systemu Cuckoo Sandbox	190
Uruchamianie API	191
Sprawdzanie stanu środowiska Cuckoo	192
Tworzenie klasy CuckooSession	193
Metody ExecuteCommand() do obsługi żądań HTTP	194
Tworzenie wieloczęściowych danych HTTP za pomocą metody GetMultipartFormData()	196
Przetwarzanie danych z pliku za pomocą klasy FileParameter	198
Testowanie klasy CuckooSession i klas pomocniczych	199
Klasa CuckooManager	201
Metoda CreateTask()	201
Szczegóły zadania i metody tworzenia raportów	203
Tworzenie abstrakcyjnej klasy Task	204
Sortowanie i tworzenie różnych typów klas	205
Połączenie elementów ze sobą	207
Testowanie aplikacji	209
Podsumowanie	211

9

AUTOMATYZACJA SQLMAP	213
Uruchamianie sqlmap	214
Interfejs API REST programu sqlmap	215
Testowanie API programu sqlmap za pomocą curl	216
Tworzenie sesji dla programu sqlmap	220
Tworzenie metody do wykonywania żądań GET	221
Wykonywanie żądania POST	222
Testowanie klasy obsługi sesji	223
Klasa SqlmapManager	225
Lista opcji sqlmap	227
Tworzenie metod realizujących skanowanie	229
Nowa metoda Main()	230
Raport ze skanowania	231
Automatyzowanie pełnego skanu sqlmap	232
Integracja sqlmap z fuzzerem SOAP	234
Dodanie obsługi żądań GET do fuzzera SOAP	235
Dodanie obsługi żądań POST do programu sqlmap	236
Wywoływanie nowych metod	238
Podsumowanie	240

10

AUTOMATYZACJA CLAMAV	241
Instalacja programu ClamAV	242
Natywna biblioteka ClamAV kontra demon sieciowy clamd	243
Automatyzacja z wykorzystaniem natywnych bibliotek ClamAV	244
Pomocnicze enumeracje i klasy	244
Dostęp do funkcji natywnej biblioteki ClamAV	247
Kompilacja silnika programu ClamAV	248

Skanowanie plików	250
Sprzątanie	252
Testowanie programu przez skanowanie pliku EICAR	252
Automatyzacja z wykorzystaniem demona clamd	254
Instalacja demona clamd	254
Uruchamianie demona clamd	255
Tworzenie klasy obsługi sesji dla demona clamd	255
Tworzenie klasy menedżera demona clamd	257
Testowanie z wykorzystaniem demona clamd	258
Podsumowanie	259

11

AUTOMATYZACJA METASPLOIT	261
Uruchamianie serwera RPC	262
instalacja Metasploitable	263
Pobranie biblioteki MSGPACK	264
instalowanie menedżera pakietów NuGet w środowisku MonoDevelop	264
Instalacja biblioteki MSGPACK	265
Dodanie referencji do biblioteki MSGPACK	266
Klasa MetasploitSession	267
Tworzenie metody Execute() dla żądań HTTP i interakcje z biblioteką MSGPACK	268
Przekształcanie danych odpowiedzi z formatu MSGPACK	270
Testowanie klasy sesji	272
Klasa MetasploitManager	273
Scalamy komponenty w całość	275
Uruchamianie eksploita	276
Interakcje z powłoką	277
Pobieranie powłok	278
Podsumowanie	279

12

AUTOMATYZACJA ARACHNI	281
Instalacja Arachni	281
Interfejs API REST systemu Arachni	282
Tworzenie klasy Arachni HTTPSession	284
Tworzenie klasy ArachniHTTPManager	285
Połączenie klas sesji i menedżera	286
RPC systemu Arachni	287
Ręczne uruchamianie mechanizmu RPC	288
Klasa ArachniRPCSession	290
Metody pomocnicze operacji ExecuteCommand()	292
Metoda ExecuteCommand()	293
Klasa ArachniRPCManager	296
Scalamy komponenty w całość	297
Podsumowanie	300

13

DEKOMPILACJA I INŻYNIERIA WSTECZNA ZARZĄDZANYCH ZESTAWÓW	301
Dekompilacja zestawów zarządzanych	302

Testowanie dekompilatora	305
Wykorzystanie narzędzia monodis do analizowania zestawu	306
Podsumowanie	309
14	
CZYTANIE GAŁĘZI REJESTRU W TRYBIE OFFLINE	311
Struktura gałęzi rejestru	312
Pobieranie gałęzi rejestru	313
Czytanie gałęzi rejestru	314
Klasa do parsowania pliku gałęzi rejestru	315
Tworzenie klasy reprezentującej klucze węzłów	316
Implementacja klasy do przechowywania kluczy wartości	321
Testowanie biblioteki	322
Zrzucanie klucza Boot	323
Metoda GetBootKey()	323
Metoda GetValueKey()	325
Metoda GetNodeKey()	325
Metoda StringToByteArray()	326
Uzyskanie klucza rozruchowego	327
Weryfikacja klucza rozruchowego	327
Podsumowanie	328
SKOROWIDZ	331