

Spis treści

O autorze	17
O recenzentach	17
Przedmowa	19
Wstęp	21
CZĘŚĆ 1. Podstawy PowerShella	
ROZDZIAŁ 1	
Pierwsze kroki z PowerShellem	29
Wymagania techniczne	29
Czym jest PowerShell?	30
Historia powłoki PowerShell	30
Dlaczego powłoka PowerShell jest tak użyteczna w kontekście cyberbezpieczeństwa?	32
Rozpoczęcie pracy z PowerShellem	36
Wprowadzenie do programowania zorientowanego obiektowo (OOP)	36
Windows PowerShell	41
PowerShell Core	42
Polityka wykonywania skryptów (Execution Policy)	47
System pomocy	53
Wersje PowerShella	58
Edytory skryptów powłoki PowerShell	61
Podsumowanie	65
Gdzie warto zajrzeć?	65
ROZDZIAŁ 2	
Podstawy skryptów PowerShell	67
Wymagania techniczne	67
Zmienne	68
Typy danych	68
Zmienne automatyczne	71

Zmienne środowiskowe	72
Słowa zastrzeżone i słowa kluczowe	72
Zasięg zmiennych	73
Operatory	76
Operatory arytmetyczne	76
Operatory porównania	77
Operatory przypisania	79
Operatory logiczne	80
Struktury sterujące	81
Warunki	81
Pętle i iteracje	84
Konwencje nazewnictwa	88
Wyszukiwanie zatwierdzonych czasowników	89
Profile PowerShell	90
Dyski PSDrives w PowerShellu	92
Tworzenie kodu wielokrotnego użytku	93
Polecenia cmdlet	93
Funkcje	94
Różnica między poleceniami cmdlet a funkcjami zaawansowanymi	98
Aliaszy	99
Moduły	102
Podsumowanie	108
Gdzie warto zajrzeć?	108
ROZDZIAŁ 3	
Technologie PowerShell Remote Management i PSRemoting	109
Wymagania techniczne	110
Praca zdalna z PowerShellem	110
PowerShell Remoting przy użyciu WinRM	111
Windows Management Instrumentation (WMI) i Common	
Information Model (CIM)	112
Open Management Infrastructure (OMI)	115

PowerShell Remoting przy użyciu SSH	115
Włączanie PowerShell Remoting	118
Ręczne włączanie PowerShell Remoting	119
Konfigurowanie PowerShell Remoting za pomocą zasad grupy (Group Policy)	124
Punkty końcowe PowerShell (konfiguracje sesji)	131
Łączenie się z określonym punktem końcowym	132
Tworzenie niestandardowego punktu końcowego — spojrzenie na JEA ...	133
Uwierzytelnianie i kwestie bezpieczeństwa PowerShell Remoting	135
Uwierzytelnianie	136
Protokoły uwierzytelniania	140
Zagadnienia związane z bezpieczeństwem uwierzytelniania typu Basic	142
Kradzież poświadczeń w kontekście PowerShell Remoting	145
Wykonywanie poleceń przy użyciu PowerShell Remoting	146
Wykonywanie pojedynczych poleceń i bloków skryptów	147
Praca z sesjami PowerShell	147
Najlepsze praktyki	151
Podsumowanie	152
Gdzie warto zajrzeć?	153
ROZDZIAŁ 4	
Wykrywanie — audyt i monitorowanie	156
Wymagania techniczne	158
Konfigurowanie rejestrowania zdarzeń PowerShell	158
Logowanie działania modułów PowerShell	158
Rejestrowanie działania bloków skryptów PowerShell	161
Chronione rejestrowanie zdarzeń	165
Transkrypcje PowerShell	167
Analiza dzienników zdarzeń	173
Wyszukiwanie dzienników zdarzeń dostępnych w systemie	174
Ogólne zapytania dotyczące zdarzeń	175
Jaki kod został wykonany w systemie?	178

Ataki typu downgrade	179
EventList	181
Wprowadzenie do rejestrowania zdarzeń	187
Przegląd najważniejszych dzienników zdarzeń związanych z PowerShellem	188
Zwiększanie maksymalnego rozmiaru dziennika	199
Podsumowanie	200
Gdzie warto zajrzeć?	200
CZĘŚĆ 2. Odkrywamy tajemnice — AD/AAD, tożsamości, dostęp do systemu i codzienne zadania związane z bezpieczeństwem	
ROZDZIAŁ 5	
PowerShell to narzędzie o ogromnych możliwościach — dostęp do systemu i interfejsów API	205
Wymagania techniczne	206
Wprowadzenie do rejestru systemu Windows	206
Praca z rejestrem	207
Scenariusze użycia rejestru w kontekście bezpieczeństwa	211
Uprawnienia użytkownika	214
Konfiguracja praw dostępu użytkownika	214
Minimalizacja ryzyka poprzez nadawanie uprawnień do tworzenia kopii zapasowych i przywracania danych	215
Delegowanie i personifikacja	216
Zapobieganie fałszowaniu dzienników zdarzeń	217
Zapobieganie kradzieży poświadczeń i atakom z wykorzystaniem pakietu Mimikatz	217
Dostęp do systemu i domeny	218
Zmiana ustawień czasu systemowego	218
Sprawdzanie i konfigurowanie uprawnień użytkownika	219
Podstawy interfejsu Windows API	222
Wprowadzenie do .NET Framework	224

.NET Framework a .NET Core	226
Kompilacja kodu C# przy użyciu .NET Framework	227
Zastosowanie polecenia Add-Type do bezpośredniej interakcji z .NET	228
Ładowanie niestandardowej biblioteki DLL z poziomu PowerShella	230
Wywoływanie Windows API za pomocą mechanizmu P/Invoke	232
Model COM i zagrożenia związane z przechwytywaniem COM	233
Ataki typu COM hijacking	235
Common Information Model (CIM)/WMI	239
Przestrzenie nazw	240
Dostawcy	242
Subskrypcje zdarzeń	245
Monitorowanie subskrypcji zdarzeń WMI/CIM	250
Manipulowanie instancjami CIM	252
Enumeracja	253
Gdzie znajduje się baza danych WMI/CIM?	255
Uruchamianie PowerShella bez powershell.exe	255
Używanie istniejących narzędzi do wywoływania funkcji zestawów	256
Binarne pliki wykonywalne	257
Wykonywanie poleceń PowerShell z poziomu .NET Framework przy użyciu C#	258
Podsumowanie	259
Gdzie warto zajrzeć?	259
ROZDZIAŁ 6	
Active Directory — ataki i przeciwdziałanie	262
Wymagania techniczne	263
Wprowadzenie do Active Directory w kontekście bezpieczeństwa	263
Jak przebiegają ataki w środowisku korporacyjnym?	264
ADSI, akceleratorzy ADSI, LDAP i przestrzeń nazw System.DirectoryServices	265
Wyliczanie	267
Wyliczanie kont użytkowników	269
Wyliczanie obiektów GPO	270

Wyliczanie grup	272
Konta i grupy uprzywilejowane	273
Wbudowane grupy uprzywilejowane w usłudze AD	273
Ataki typu password spraying	276
Zapobieganie atakom	276
Prawa dostępu	278
Czym jest identyfikator SID?	278
Listy kontroli dostępu	279
Listy ACL dla jednostek OU	280
GPO ACL	283
Listy ACL dla domeny	284
Relacje zaufania domen	286
Kradzież danych uwierzytelniających	287
Protokoły uwierzytelniania	287
Atakowanie uwierzytelniania AD — kradzież danych uwierzytelniających i ruchy boczne	292
Zapobieganie	302
Konfiguracje bazowe i zestaw narzędzi Microsoft Security Compliance Toolkit	304
Podsumowanie	305
Gdzie warto zajrzeć?	306
ROZDZIAŁ 7	
Hakowanie w chmurze — wykorzystywanie luk i podatności w Azure Active Directory (Entra ID)	308
Wymagania techniczne	309
Różnice między AD a AAD	309
Uwierzytelnianie w AAD	311
Tożsamość urządzenia — łączenie urządzeń z AAD	311
Tożsamości hybrydowe	311
Protokoły i koncepcje	313
Uprzywilejowane konta i role	319

Dostęp do AAD z poziomu PowerShella	321
Azure CLI	322
Azure PowerShell	323
Ataki na Azure AD	325
Anonimowe wyliczanie kont i zasobów AAD	326
Ataki typu password spraying	328
Uwierzytelnione wyliczanie kont i zasobów AAD	329
Kradzież danych uwierzytelniających	335
Kradzież tokenów	336
Atak typu wyrażenie zgody — trwały dostęp dzięki uprawnieniom aplikacji	342
Nadużywanie jednokrotnego logowania (SSO) w Azure AD	343
Ataki na uwierzytelnianie typu pass-through (PTA)	344
Środki zaradcze	345
Podsumowanie	347
Gdzie warto zajrzeć?	348
ROZDZIAŁ 8	
Zadania i poradnik operacyjny dla zespołów Red Team	350
Wymagania techniczne	350
Fazy ataków	350
Narzędzia PowerShell dla zespołów Red Team	352
PowerSploit	352
Invoke-Mimikatz	354
Empire	354
Inveigh	355
PowerUpSQL	355
AADInternals	356
Red Team Cookbook — poradnik operacyjny	356
Rekonesans	357
Wykonanie	357
Trwałość	364

Unikanie wykrycia	368
Dostęp do danych uwierzytelniających	372
Odkrywanie	373
Ruch boczny	376
Command and Control (C2)	377
Eksfiltracja	379
Uderzenie	379
Podsumowanie	380
Gdzie warto zajrzeć?	381
ROZDZIAŁ 9	
Zadania i poradnik operacyjny dla zespołów Blue Team	382
Wymagania techniczne	382
Ochrona, wykrywanie i reagowanie	383
Ochrona	383
Wykrywanie	384
Reagowanie	385
Popularne narzędzia PowerShell dla zespołów Blue Team	385
PSGumshoe	385
PowerShellArsenal	386
AtomicTestHarnesses	386
PowerForensics	387
NtObjectManager	387
DSInternals	387
PSScriptAnalyzer i InjectionHunter	388
Revoke-Obfuscation	388
Posh-VirusTotal	389
EventList	389
JEAnalyzer	390
Blue Team Cookbook — poradnik operacyjny	390
Sprawdzanie zainstalowanych aktualizacji	390
Sprawdzanie brakujących aktualizacji	391

Przeglądanie historii poleceń PowerShell wszystkich użytkowników	391
Sprawdzanie dziennika zdarzeń zdalnego hosta	392
Monitorowanie wykonywania poleceń PowerShell z pominięciem powershell.exe	393
Przeglądanie wybranych reguł zapory sieciowej	394
Ograniczenie komunikacji PowerShell do prywatnych zakresów adresów IP	395
Izolowanie zagrożonego systemu	395
Zdalne sprawdzanie zainstalowanego oprogramowania	396
Uruchamianie transkrypcji PowerShell	396
Sprawdzanie ważności certyfikatów	397
Weryfikacja podpisu cyfrowego pliku lub skryptu	398
Sprawdzanie praw dostępu do plików i folderów	398
Wyświetlanie listy wszystkich uruchomionych usług	400
Zatrzymywanie usług	400
Wyświetlanie wszystkich procesów	400
Zatrzymywanie procesów	401
Wyłączanie konta lokalnego	401
Włączanie konta lokalnego	402
Wyłączanie konta domenowego	402
Włączanie konta domenowego	402
Wyświetlanie wszystkich ostatnio utworzonych kont domenowych	403
Sprawdzanie, czy wybrany port jest otwarty	403
Wyświetlanie połączeń TCP i ich procesów inicjujących	404
Wyświetlanie połączeń UDP i ich procesów inicjujących	404
Wykrywanie ataków typu downgrade przy użyciu dziennika zdarzeń systemu Windows	405
Zapobieganie atakom typu downgrade	405
Podsumowanie	406
Gdzie warto zajrzeć?	406
CZĘŚĆ 3. Zabezpieczanie PowerShella	

— skuteczne metody ochrony

ROZDZIAŁ 10

Tryby językowe sesji PowerShell i technologia JEA	411
Wymagania techniczne	412
Czym są tryby językowe w PowerShellu?	412
Tryb Full Language	412
Tryb Restricted Language	412
Tryb No Language	413
Tryb Constrained Language	413
Czym jest JEA?	415
Wprowadzenie do JEA	415
Planowanie wdrożenia JEA	417
Plik definicji roli	418
Plik konfiguracji sesji	426
Wdrażanie JEA	434
Nawiązywanie połączenia z sesją JEA	436
Upraszczanie wdrożenia JEA przy użyciu modułu JEAnalyzer	437
Konwersja skryptów na konfigurację JEA	438
Wykorzystanie audytu do utworzenia początkowej konfiguracji JEA	439
Rejestrowanie zdarzeń w sesjach JEA	440
Transkrypcja na żywo	440
Dzienniki zdarzeń PowerShell	440
Inne dzienniki zdarzeń	441
Najlepsze praktyki — minimalizowanie zagrożeń i podatności	442
Podsumowanie	443
Gdzie warto zajrzeć?	444

ROZDZIAŁ 11

AppLocker, kontrolowanie aplikacji i podpisywanie kodu	445
Wymagania techniczne	445
Zapobieganie nieautoryzowanemu wykonywaniu skryptów za pomocą podpisywania kodu	446

Kontrolowanie aplikacji i skryptów	453
Planowanie kontroli aplikacji	454
Wbudowane rozwiązania do kontroli aplikacji	455
Pierwsze kroki z Microsoft AppLocker	457
Wdrażanie funkcji AppLocker	458
Audyt zdarzeń AppLocker	469
Odkrywamy technologię Windows Defender Application Control	470
Tworzenie zasad integralności kodu	471
Bezpieczeństwo oparte na wirtualizacji (VBS)	477
Wdrażanie WDAC	479
Jak zmienia się działanie PowerShella, gdy włączona jest kontrola aplikacji?	481
Podsumowanie	483
Gdzie warto zajrzeć?	484
ROZDZIAŁ 12	
Tajniki interfejsu AMSI	486
Wymagania techniczne	486
Czym jest AMSI i jak to działa?	487
Dlaczego AMSI? Praktyczny przykład	488
Przykład 1.	490
Przykład 2.	490
Przykład 3.	490
Przykład 4.	491
Przykład 5.	491
Przykład 6.	492
Omijanie mechanizmu AMSI	493
Zapobieganie wykrywaniu plików lub tymczasowe wyłączenie AMSI ...	495
Zaciemnianie kodu	501
Kodowanie Base64	503
Podsumowanie	504
Gdzie warto zajrzeć?	504

ROZDZIAŁ 13

Co jeszcze warto wiedzieć? Dodatkowe metody

ochrony i inne przydatne zasoby	506
Wymagania techniczne	506
Bezpieczne skrypty	506
PSScriptAnalyzer	507
InjectionHunter	508
Poznajemy konfigurację żądanego stanu	509
DSC 1.1	510
DSC 2.0	511
DSC 3.0	511
Konfiguracja	512
Utwarczanie systemów i środowisk	513
Bazowe konfiguracje zabezpieczeń	513
Instalacja aktualizacji zabezpieczeń i monitorowanie	
zgodności poprawek	519
Zapobieganie ruchowi bocznemu	521
Uwierzytelnianie wieloskładnikowe przy podnoszeniu uprawnień	522
Czasowo ograniczone uprawnienia (administracja na żądanie)	523
Wykrywanie ataków — identyfikacja i reakcja na zagrożenia	
w punktach końcowych	523
Aktywacja darmowych funkcji ochrony punktów końcowych	
Microsoft Defender	524
Podsumowanie	524
Gdzie warto zajrzeć?	524
Skorowidz	527