

# Spis treści

.....	17
.....	19
.....	21
<b>Część I</b>	
<b>PRZEGLĄD SYSTEMU OPERACYJNEGO WINDOWS</b>	
<b>1</b>	<b>31</b>
<b>KONFIGUROWANIE ŚRODOWISKA TESTOWEGO NARZĘDZIA POWERSHELL</b>	<b>31</b>
Wybór wersji narzędzia PowerShell	31
Konfigurowanie narzędzia PowerShell	32
Przegląd języka narzędzia PowerShell	33
Typy, zmienne i wyrażenia	33
Wykonywanie poleceń	37
Znajdowanie poleceń i uzyskiwanie pomocy	38
Definiowanie funkcji	42
Wyświetlanie i modyfikowanie obiektów	43
Filtrowanie, sortowanie i grupowanie obiektów	46
Eksportowanie danych	49
Podsumowanie	50
<b>2</b>	<b>51</b>
<b>JĄDRO SYSTEMU WINDOWS</b>	<b>51</b>
Obszar wykonawczy jądra systemu Windows	52
Monitor referencyjny zabezpieczeń	53
Menedżer obiektów	55
Typy obiektów	55
Przestrzeń nazw menedżera obiektów	56
Wywołania systemowe	58
Kody NTSTATUS	62

Uchwyty obiektów .....	64
Informacyjne wywołania systemowe Query i Set .....	72
Menedżer operacji wejścia-wyjścia .....	75
Menedżer procesów i wątków .....	77
Menedżer pamięci .....	78
Polecenia NtVirtualMemory .....	79
Obiekty Section .....	81
Integralność kodu .....	84
Zaawansowane lokalne wywoływanie procedur .....	85
Menedżer konfiguracji .....	85
Praktyczne przykłady .....	87
Znajdowanie otwartych uchwytów na podstawie nazwy .....	87
Znajdowanie współużytkowanych obiektów .....	88
Modyfikowanie mapowanej sekcji .....	89
Znajdowanie pamięci umożliwiającej zapis i wykonywanie .....	91
Podsumowanie .....	92
<b>3</b>	
<b>APLIKACJE TRYBU UŻYTKOWNIKA .....</b>	<b>93</b>
Interfejsy API podsystemu Win32 i trybu użytkownika systemu Windows .....	94
Ładowanie nowej biblioteki .....	95
Wyświetlanie zaimportowanych interfejsów API .....	96
Wyszukiwanie bibliotek DLL .....	98
Graficzny interfejs użytkownika podsystemu Win32 .....	100
Zasoby jądra związane z graficznym interfejsem użytkownika .....	102
Komunikaty okien .....	104
Sesje konsoli .....	105
Porównanie interfejsów API i wywołań systemowych podsystemu Win32 .....	108
Ścieżki rejestru podsystemu Win32 .....	111
Otwieranie kluczy .....	112
Wyświetlanie zawartości rejestru .....	113
Ścieżki urządzeń systemu DOS .....	114
Typy ścieżek .....	115
Maksymalne długości ścieżki .....	117
Tworzenie procesów .....	119
Analizowanie wiersza poleceń .....	120
Interfejsy API powłoki .....	121
Procesy systemowe .....	124
Menedżer sesji .....	124
Proces logowania w systemie Windows .....	124
Podsystem autoryzacji LSASS .....	125
Menedżer kontroli usług .....	125

Praktyczne przykłady .....	126
Znajdowanie plików wykonywalnych importujących konkretne interfejsy API .....	126
Znajdowanie ukrytych kluczy lub wartości rejestru .....	127
Podsumowanie .....	129

## Część II

### MONITOR SRM

<b>4</b>		
<b>TOKENY DOSTĘPU BEZPIECZEŃSTWA .....</b>		<b>133</b>
Tokeny podstawowe .....		134
Tokeny personifikacji .....		138
Opcja SQoS .....		139
Jawna personifikacja tokena .....		141
Przekształcanie typów tokenów .....		142
Pseudouchwyty tokenów .....		143
Grupy tokenów .....		144
Flagi Enabled, EnabledByDefault i Mandatory .....		145
Flaga LogonId .....		145
Flaga Owner .....		146
Flaga UseForDenyOnly .....		146
Flagi Integryty i IntegrityEnabled .....		147
Flaga Resource .....		148
Grupy urzędzeń .....		148
Uprawnienia .....		149
Tokeny „piaskownicy” .....		152
Tokeny ograniczone .....		153
Tokeny z ograniczeniem zapisu .....		155
AppContainer i tokeny lowbox .....		155
Co czyni użytkownika administratorem? .....		159
Kontrola konta użytkownika .....		161
Tokeny powiązane i typ zwiększania uprawnień .....		163
Dostęp do interfejsu użytkownika .....		166
Wirtualizacja .....		167
Atrybuty zabezpieczeń .....		167
Tworzenie tokenów .....		169
Przypisywanie tokena .....		171
Przypisywanie tokena podstawowego .....		171
Przypisywanie tokena personifikacji .....		174

Praktyczne przykłady .....	176
Znajdowanie procesów z dostępem do interfejsu użytkownika .....	177
Znajdowanie uchwytów tokenów poddawanych personifikacji .....	177
Usuwanie uprawnień administratora .....	178
Podsumowanie .....	179
<b>5</b>	
<b>DESKRYPTORY ZABEZPIECZEŃ .....</b>	<b>180</b>
Struktura deskryptora zabezpieczeń .....	181
Struktura identyfikatora SID .....	183
Bezwzględne i względne deskryptory zabezpieczeń .....	186
Nagłówki i wpisy listy kontroli dostępu .....	189
Nagłówek .....	189
Lista wpisów ACE .....	190
Tworzenie deskryptorów zabezpieczeń i modyfikowanie ich .....	194
Tworzenie nowego deskryptora zabezpieczeń .....	195
Uporządkowanie wpisów ACE .....	196
Formatowanie deskryptorów zabezpieczeń .....	197
Przekształcanie dotyczące względnego deskryptora zabezpieczeń .....	202
Język SDDL .....	202
Praktyczne przykłady .....	212
Ręczne analizowanie binarnego identyfikatora SID .....	212
Wyliczanie identyfikatorów SID .....	214
Podsumowanie .....	215
<b>6</b>	
<b>ODCZYTYWANIE I PRZYPISYWANIE DESKRYPTORÓW ZABEZPIECZEŃ .....</b>	<b>217</b>
Odczytywanie deskryptorów zabezpieczeń .....	218
Przypisywanie deskryptorów zabezpieczeń .....	220
Przypisywanie deskryptora zabezpieczeń podczas tworzenia zasobu .....	220
Przypisywanie deskryptora zabezpieczeń do istniejącego zasobu .....	247
Interfejsy API zabezpieczeń podsystemu Win32 .....	250
Deskryptory zabezpieczeń serwera i złożone wpisy ACE .....	256
Podsumowanie sposobu dziedziczenia .....	257
Praktyczne przykłady .....	259
Znajdowanie właścicieli zasobów menedżera obiektów .....	259
Zmiana właściciela zasobu .....	261
Podsumowanie .....	263

<b>7</b>	<b>PROCES KONTROLI DOSTĘPU</b>	<b>264</b>
	Przeprowadzanie kontroli dostępu	264
	Kontrole dostępu w trybie jądra	265
	Kontrole dostępu w trybie użytkownika	268
	Polecenie Get-NtGrantedAccess narzędzia PowerShell	269
	Proces kontroli dostępu w narzędziu PowerShell	270
	Definiowanie funkcji kontroli dostępu	271
	Przeprowadzanie obowiązkowej kontroli dostępu	273
	Wykonywanie kontroli dostępu tokena	281
	Przeprowadzanie uznaniowej kontroli dostępu	285
	Izolowanie w „piaskownicy”	288
	Tokeny ograniczone	288
	Tokeny lowbox	290
	Kontrole dostępu w przedsiębiorstwach	294
	Kontrola dostępu dotycząca typu obiektu	294
	Centralna zasada dostępu	300
	Praktyczne przykłady	306
	Zastosowanie funkcji Get-PSGrantedAccess	306
	Obliczanie przyznanego poziomu dostępu dla zasobów	308
	Podsumowanie	309
<b>8</b>	<b>INNE PRZYPADKI ZASTOSOWANIA KONTROLI DOSTĘPU</b>	<b>310</b>
	Kontrola z przechodzeniem	311
	Uprawnienie SeChangeNotifyPrivilege	312
	Ograniczone kontrole	313
	Kontrole dostępu podczas duplikowania uchwytów	315
	Kontrole tokenów „piaskownicy”	318
	Automatyzowanie kontroli dostępu	320
	Praktyczne przykłady	324
	Uproszczenie kontroli dostępu dla obiektu	324
	Znajdowanie obiektów Section z możliwością zapisu	324
	Podsumowanie	326
<b>9</b>	<b>AUDYT ZABEZPIECZEŃ</b>	<b>327</b>
	Dziennik zdarzeń zabezpieczeń	327
	Konfigurowanie systemowej zasady audytu	328
	Konfigurowanie zasady audytu dla poszczególnych użytkowników	331
	Zabezpieczenia zasad audytu	333
	Konfigurowanie listy SAFL zasobu	334
	Konfigurowanie globalnej listy SAFL	339

Praktyczne przykłady .....	340
Weryfikowanie zabezpieczeń zasady audytu .....	340
Znajdowanie zasobów z wpisami ACE typu Audit .....	341
Podsumowanie .....	342

### **CZĘŚĆ III**

## **UWIERZYTELNIANIE I AUTORYZACJA W RAMACH ZABEZPIECZEŃ LOKALNYCH**

<b>10</b>	
<b>UWIERZYTELNIANIE W SYSTEMIE WINDOWS .....</b>	<b>345</b>
Uwierzytelnianie domenowe .....	346
Uwierzytelnianie lokalne .....	346
Domena sieci korporacyjnej .....	347
Lasy domen .....	348
Konfiguracja domeny lokalnej .....	351
Baza danych użytkowników .....	351
Baza danych zasad jednostki autoryzacji LSA .....	356
Zdalne usługi LSA .....	358
Zdalna usługa menedżera SAM .....	359
Usługa zdalna zasady domeny .....	366
Baza danych menedżera SAM i baza SECURITY .....	372
Uzyskiwanie dostępu do bazy danych menedżera SAM za pośrednictwem rejestru .....	373
Inspekcja bazy danych SECURITY .....	383
Praktyczne przykłady .....	385
Cykliczne stosowanie identyfikatorów RID .....	385
Wymuszanie zmiany hasła użytkownika .....	386
Wyodrębnianie skrótów wszystkich użytkowników lokalnych .....	387
Podsumowanie .....	388
<b>11</b>	
<b>USŁUGA ACTIVE DIRECTORY .....</b>	<b>390</b>
Krótką historia usługi Active Directory .....	390
Eksploracja domeny usługi Active Directory za pomocą narzędzia PowerShell .....	391
Narzędzia administracji zdalnej serwera .....	391
Podstawowe informacje o lesie i domenie .....	393
Użytkownicy .....	394
Grupy .....	395
Komputery .....	397
Obiekty i nazwy wyróżniające .....	398
Wyliczanie obiektów katalogu .....	399
Uzyskiwanie dostępu do obiektów w innych domenach .....	401

Schemat .....	402
Inspekcja schematu .....	404
Uzyskiwanie dostępu do atrybutów zabezpieczeń .....	405
Deskryptory zabezpieczeń .....	407
Tworzenie zapytań dotyczących deskryptorów zabezpieczeń obiektów katalogu .....	408
Przypisywanie deskryptorów zabezpieczeń nowym obiektom katalogu .....	410
Przypisywanie deskryptorów zabezpieczeń istniejącym obiektom .....	413
Inspekcja odziedziczonych zabezpieczeń deskryptora .....	415
Kontrola dostępu .....	416
Tworzenie obiektów .....	417
Usuwanie obiektów .....	419
Wyszczególnianie obiektów .....	419
Odczyt i zapis atrybutów .....	420
Sprawdzanie wielu atrybutów .....	421
Analizowanie zestawów właściwości .....	423
Inspekcja praw dostępu kontroli .....	427
Analizowanie praw dostępu z potwierdzonym zapisem .....	429
Uzyskiwanie dostępu do identyfikatora SID konta SELF .....	430
Wykonywanie dodatkowych kontroli zabezpieczeń .....	431
Oświadczenia i centralne zasady dostępu .....	434
Zasady grup .....	435
Praktyczny przykład .....	438
Budowanie kontekstu autoryzacji .....	438
Zbieranie informacji o obiekcie .....	442
Wykonywanie kontroli dostępu .....	443
Podsumowanie .....	447
<b>12</b>	
<b>UWIERZYTELNIANIE INTERAKTYWNE .....</b>	<b>449</b>
Tworzenie pulpitu użytkownika .....	450
Interfejs API LsaLogonUser .....	451
Uwierzytelnianie lokalne .....	453
Uwierzytelnianie w domenie .....	455
Sesje logowania i konsoli .....	457
Tworzenie tokena .....	459
Użycie interfejsu API LsaLogonUser z poziomu narzędzia PowerShell .....	462
Tworzenie nowego procesu za pomocą tokena .....	465
Typ logowania Service .....	466
Praktyczne przykłady .....	467
Testowanie uprawnień i praw kont logowania .....	467
Tworzenie procesu w innej sesji konsoli .....	469
Uwierzytelnianie kont wirtualnych .....	471
Podsumowanie .....	472

<b>13</b>	<b>UWIERZYTELNIANIE SIECIOWE .....</b>	<b>474</b>
	Uwierzytelnianie sieciowe za pomocą protokołu NTLM .....	475
	Uwierzytelnianie oparte na protokole NTLM z wykorzystaniem narzędzia PowerShell .....	476
	Proces przekształcania kryptograficznego .....	484
	Uwierzytelnianie z przekazywaniem .....	487
	Uwierzytelnianie z użyciem lokalnej pętli zwrotnej .....	488
	Alternatywne dane uwierzytelniające klienta .....	490
	Atak NTLM Relay .....	492
	Schemat ataku .....	492
	Aktywne wyzwania serwera .....	494
	Podpisywanie i uszczelnianie .....	494
	Nazwy elementów docelowych .....	497
	Powiązanie kanału .....	498
	Praktyczny przykład .....	499
	Przegląd .....	499
	Moduł kodu .....	500
	Implementacja serwera .....	503
	Implementacja klienta .....	505
	Test uwierzytelniania za pomocą protokołu NTLM .....	507
	Podsumowanie .....	509
<b>14</b>	<b>PROTOKÓŁ KERBEROS .....</b>	<b>510</b>
	Uwierzytelnianie interaktywne z użyciem protokołu Kerberos .....	511
	Początkowe uwierzytelnianie użytkownika .....	511
	Uwierzytelnianie w usługach sieciowych .....	516
	Realizowanie w narzędziu PowerShell procesu uwierzytelniania protokołu Kerberos .....	519
	Odszyfrowywanie komunikatu żądania AP-REQ .....	522
	Odszyfrowywanie komunikatu odpowiedzi AP-REP .....	530
	Uwierzytelnianie między domenami .....	532
	Delegowanie w protokole Kerberos .....	534
	Delegowanie bez ograniczeń .....	535
	Delegowanie ograniczone .....	539
	Wzajemne uwierzytelnianie użytkowników za pomocą protokołu Kerberos .....	546
	Praktyczne przykłady .....	549
	Sprawdzanie pamięci podręcznej biletów protokołu Kerberos .....	549
	Prosty atak Kerberoasting .....	550
	Podsumowanie .....	552

**PAKIET UWIERZYTELNIANIA NEGOTIATE ORAZ INNE PAKIETY ZABEZPIECZEŃ ..... 553**

Bufory zabezpieczeń .....	554
Zastosowanie buforów z kontekstem uwierzytelniania .....	555
Zastosowanie buforów podczas podpisywania i zabezpieczania .....	556
Protokół Negotiate .....	557
Mniej popularne pakiety zabezpieczeń .....	559
Bezpieczny kanał .....	560
Pakiet protokołu CredSSP .....	564
Opcja Remote Credential Guard i tryb ograniczony administratora .....	567
Menedżer danych uwierzytelniających .....	568
Dodatkowe flagi atrybutów żądania .....	572
Sesje anonimowe .....	572
Tokeny tożsamości .....	573
Uwierzytelnianie sieciowe z użyciem tokena lowbox .....	575
Uwierzytelnianie z wykorzystaniem możliwości uwierzytelniania korporacyjnego .....	575
Uwierzytelnianie w znanej sieciowej usłudze proxy .....	576
Uwierzytelnianie z użyciem jawnych danych uwierzytelniających .....	577
Dziennik zdarzeń audytu uwierzytelniania .....	579
Praktyczne przykłady .....	583
Identyfikowanie przyczyny nieudanego uwierzytelniania .....	583
Zastosowanie bezpiecznego kanału do wyodrębnienia certyfikatu protokołu TLS serwera .....	586
Podsumowanie .....	588
Końcowe wnioski .....	589

**DODATEK A.****BUDOWANIE SIECI DOMEN SYSTEMU WINDOWS DO TESTÓW ..... 590**

Sieć domen .....	591
Instalowanie i konfigurowanie oprogramowania Hyper-V systemu Windows .....	592
Tworzenie maszyn wirtualnych .....	593
Serwer PRIMARYDC .....	595
Stacja robocza GRAPHITE .....	598
Serwer SALESDC .....	599

**DODATEK B.****ODWZOROWYWANIE ALIASÓW IDENTYFIKATORÓW SID FORMATU SDDL ..... 602****SKOROWIDZ ..... 607**