

Spis treści

O autorze 15

O recenzentach 17

Przedmowa 19

CZĘŚĆ I. ZAAKCEPTOWANIE CZERWONEGO ZESPOŁU 27

Rozdział 1. Uruchamianie programu bezpieczeństwa ofensywnego 29

Definiowanie misji - adwokat diabła 30

Uzyskanie poparcia kadry kierowniczej 31

Przekonywanie kierownictwa za pomocą danych 31

Przekonywanie kierownictwa za pomocą działań i wyników 32

Miejsce czerwonego zespołu w schemacie organizacyjnym 32

Droga ku przyszłości bezpieczeństwa ofensywnego 33

Tworzenie nowego programu od podstaw 33

Dziedziczenie istniejącego programu 33

Ludzie - spotkanie z członkami czerwonego zespołu 34

Dlaczego pentesterzy są tacy niesamowici? 35

Inżynieria bezpieczeństwa ofensywnego jako dyscyplina zawodowa 35

Strategiczne podejście członków czerwonych zespołów 36

Zarządzanie programami 36

Przyciąganie i zatrzymywanie talentów 36

Różnorodność i otwartość 38

Morale i tożsamość zespołu 39

Reputacja zespołu 40

Świadczenie różnych usług na rzecz organizacji 40

Wsparcie dla przeglądu zabezpieczeń i modelowania zagrożeń 41

| | |
|---|----|
| Ocena bezpieczeństwa | 41 |
| Działania zespołu czerwonego | 42 |
| Działania zespołu fioletowego | 42 |
| Ćwiczenia symulacyjne | 43 |
| Badania i rozwój | 43 |
| Predykcyjna analiza ataków i wsparcie dla reagowania na incydenty | 43 |
| Dodatkowe obowiązki programu ofensywnego | 44 |
| Edukacja i szkolenie w zakresie bezpieczeństwa | 44 |
| Zwiększenie IQ bezpieczeństwa organizacji | 44 |
| Gromadzenie informacji o zagrożeniach | 44 |
| Informowanie grup zarządzania ryzykiem i kierownictwa | 44 |
| Integracja z procesami inżynieryjnymi | 45 |
| Mam wrażenie, jakbym Cię znał - zrozumienie etycznych aspektów działań czerwonego zespołu | 45 |
| Szkolenie i edukacja zespołów bezpieczeństwa ofensywnego | 46 |
| Zasady, reguły i standardy | 47 |
| Zasady, którymi należy się kierować, i reguły, których należy przestrzegać | 47 |
| Działanie z określonym celem i zachowanie pokory | 47 |
| Testy penetracyjne są reprezentatywne, ale nie wyczerpujące | 48 |
| Pentesting nie zastępuje funkcjonalnego testowania bezpieczeństwa | 48 |
| Umożliwienie pentesterom eksploracji | 48 |
| Informowanie grup zarządzających ryzykiem | 49 |
| Zasady przeprowadzania testów penetracyjnych | 49 |
| Dostosowywanie zasad przeprowadzania testów penetracyjnych do operacji | 50 |
| Geograficzne i jurysdykcyjne obszary działania | 50 |
| Dystrybucja materiałów informacyjnych | 51 |
| Prawdziwe, symulowane i emulowane ataki | 51 |
| Porównanie systemów produkcyjnych i nieprodukcyjnych | 52 |
| Unikaj zostania pionkiem w politycznej rozgrywce | 52 |
| Standardowa procedura operacyjna | 52 |
| Wykorzystywanie planów ataków do śledzenia operacji | 53 |

| | |
|---|----|
| Cel misji - co zamierzamy osiągnąć lub zademonstrować? | 53 |
| Zainteresowane strony i ich obowiązki | 54 |
| Kryptonimy | 55 |
| Harmonogram i czas trwania | 55 |
| Ryzyko związane z testami penetracyjnymi i autoryzacja | 56 |
| Spotkanie wdrożeniowe | 56 |
| Rezultaty | 56 |
| Powiadamianie zainteresowanych stron | 57 |
| Wykonywanie planu ataku - śledzenie postępów w trakcie operacji | 57 |
| Dokumentowanie działań | 59 |
| Podsumowywanie operacji | 61 |
| Udostępnianie nadrzędnych informacji za pośrednictwem dashboardów | 64 |
| Kontaktowanie się z zespołem pentesterów i zamawianie usług | 64 |
| Modelowanie przeciwnika | 65 |
| Zrozumienie przeciwników zewnętrznych | 65 |
| Uwzględnianie zagrożeń wewnętrznych | 65 |
| Czynniki motywujące | 66 |
| Anatomia włamania | 66 |
| Ustanowienie przyczółka | 66 |
| Osiąganie celu misji | 67 |
| Włamywanie się do aplikacji internetowych | 68 |
| Słabe poświadczenia | 68 |
| Brak integralności i poufności | 68 |
| Łańcuch niszczenia intruzów Lockheeda Martina | 68 |
| Anatomia katastrofy usługi w chmurze | 69 |
| Tryby działania - operacja chirurgiczna lub nalot dywanowy | 70 |
| Działanie chirurgiczne | 70 |
| Naloty dywanowe | 70 |
| Środowisko i przestrzeń biurowa | 71 |
| Porównanie otwartej i zamkniętej przestrzeni biurowej | 71 |
| Zabezpieczenie środowiska fizycznego | 71 |

Jeśli trzeba, zbieraj najlepsze zespoły 72

Skoncentrowanie się na aktualnym zadaniu 72

Podsumowanie 72

Pytania 73

Rozdział 2. Zarządzanie zespołem bezpieczeństwa ofensywnego 75

Zrozumienie rytmu biznesowego i planowanie operacji zespołu czerwonego 76

Planowanie cykli 76

Spotkania pozazakładowe 76

Zachęcanie do różnorodnych pomysłów i unikanie myślenia grupowego 78

Planowanie operacji - skupianie się na celach 78

Planowanie operacji - skupianie się na zasobach 80

Planowanie operacji - skupianie się na lukach w zabezpieczeniach 80

Planowanie operacji - skupianie się na taktykach ataków, technikach i procedurach 81

Planowanie operacji - skupienie się na frameworku STRIDE 81

Zarządzanie zespołem i ocena jego wydajności 83

Regularne spotkania indywidualne 83

Przekazywanie złych wiadomości 83

Świętowanie sukcesu i dobra zabawa 84

Zarządzanie przez przechadzanie się 84

Zarządzanie kadrą kierowniczą 85

Zarządzanie samym sobą 85

Obsługa logistyki, spotkań i pozostawanie na obranym kursie 85

Spotkania zespołu 86

Praca zdalna 86

Ciągłe testy penetracyjne 87

Ciągłe dostosowywanie zasobów 87

Mądrze wybieraj swoje bitwy 87

Korzystanie ze wsparcia zewnętrznych firm 88

Rozwój zespołu 89

Możliwość szybkiego zatrudniania nowych pracowników 89

| | |
|---|-----|
| Doskonałość we wszystkim | 90 |
| Gotowość do przeprowadzania testów bezpieczeństwa ofensywnego | 91 |
| Budowanie laboratorium do przeprowadzania ataków | 91 |
| Kieruj zespołem i inspiruj go | 92 |
| Aby uzyskać najlepsze wyniki, pozwól na swobodę działania | 92 |
| Wykorzystanie przewagi własnego terytorium | 93 |
| Znalezienie wspólnego celu przez zespoły czerwony, niebieski i inżynierski | 93 |
| Zostałem przyłapany! Jak zbudować pomost | 95 |
| Uczenie się od siebie nawzajem, aby się doskonalić | 96 |
| Polowanie na zagrożenia | 96 |
| Rozwijanie zespołu fioletowego, aby był bardziej efektywny | 96 |
| Techniki ofensywne i defensywne środki obrony | 97 |
| Udostępnianie maszyn atakujących! | 97 |
| Aktywna obrona, honeypoty i wabiki | 98 |
| Ochrona pentestera | 99 |
| Wykonywanie ciągłej, kompleksowej walidacji testowej potoku reagowania na incydenty | 99 |
| Zwalczanie normalizacji dewiacji | 100 |
| Zachowanie zdrowego zróżnicowania poglądów między zespołami czerwonym i niebieskim | 100 |
| Przerywanie passy zespołu fioletowego | 101 |
| Podsumowanie | 101 |
| Pytania | 102 |
| | |
| Rozdział 3. Mierzenie efektywności programu bezpieczeństwa ofensywnego | 103 |
| Iluzja kontroli | 104 |
| Droga do dojrzałości | 105 |
| Strategiczne działania zespołu czerwonego w całej organizacji | 106 |
| Ryzyko związane z działaniem w trybie skrytym | 106 |
| Śledzenie ustaleń i incydentów | 107 |
| Powtarzalność | 112 |
| Automatyzacja działań zespołu czerwonego, aby pomóc obrońcom | 112 |
| Ochrona informacji - zabezpieczanie ustaleń czerwonego zespołu | 113 |

| | |
|--|-----|
| Pomiar trwałości obecności zespołu czerwonego w środowisku | 113 |
| Zmaganie się z mgłą wojny | 114 |
| Zagrożenia - drzewa i grafy | 115 |
| Ręczne tworzenie grafów koncepcyjnych | 115 |
| Automatyzowanie wykrywania i umożliwienie eksploracji | 118 |
| Definiowanie wskaźników oraz kluczowych wskaźników efektywności | 120 |
| Śledzenie podstawowych zobowiązań wewnętrznych zespołu | 120 |
| Dashboards ze statystykami ataków - badanie wskaźników bojowych | 121 |
| Punktacja zespołu czerwonego | 123 |
| Śledzenie dotkliwości ustaleń i pomiar ryzyka | 128 |
| Wyjście poza skale porządkowe | 128 |
| Korzystanie ze wskaźników średniego czasu | 129 |
| Eksperymentowanie z symulacjami metodą Monte Carlo | 130 |
| Macierz reagowania na zagrożenia | 134 |
| Framework Test Maturity Model integration i działania czerwonego zespołu | 135 |
| Poziom 1. - wstępny | 135 |
| Poziom 2. - zarządzany | 135 |
| Poziom 3. - zdefiniowany | 136 |
| Poziom 4. - mierzony | 136 |
| Poziom 5. - optymalizacja | 137 |
| Poziom 6. - iluzja kontroli, czyli zespół czerwony kontratakuje | 137 |
| Macierz ATT&CK firmy MITRE | 137 |
| ATT&CK Navigator | 138 |
| Pamiętaj, na czym polega działanie zespołu czerwonego | 141 |
| Podsumowanie | 141 |
| Pytania | 142 |
| | |
| Rozdział 4. Progresywne operacje zespołu czerwonego | 143 |
| Badanie różnych rodzajów działań operacyjnych w cyberprzestrzeni | 144 |
| Wydobywanie kryptowalut | 145 |

Wydobywanie kryptowalut, aby zademonstrować wpływ finansowy, czyli kiedy lecimy na Księżyc? 146

Działania zespołu czerwonego w celu ochrony danych osobowych 149

Pierwsze kroki w testowaniu skoncentrowanym na naruszeniach poufności danych osobowych 150

Wysyłanie symulowanego rachunku do wewnętrznych zespołów 152

Przeprowadzanie testów penetracyjnych zespołu czerwonego 153

Obranie za cel niebieskiego zespołu 154

Wykorzystanie systemów ochrony punktów końcowych zespołu niebieskiego jako C2 154

Media społecznościowe i reklama ukierunkowana 155

Falszowanie danych telemetrycznych w celu zmanipulowania rozwoju nowych funkcjonalności oprogramowania 156

Atakowanie sztucznej inteligencji i systemów uczenia maszynowego 156

Operacja "Straż obywatelska" - wykorzystanie zespołu czerwonego do wdrażania poprawek 157

Emulowanie rzeczywistych ATP 158

Przeprowadzanie ćwiczeń symulowanych 158

Angażowanie w ćwiczenia zespołu kierowniczego 160

Podsumowanie 160

Pytania 161

CZĘŚĆ II. TAKTYKI I TECHNIKI 163

Rozdział 5. Świadomość sytuacyjna - mapowanie własnego terytorium za pomocą grafowych baz danych 165

Grafy ataków i wiedzy 166

Podstawy grafowej bazy danych 167

Węzły lub wierzchołki 168

Relacje lub krawędzie 168

Właściwości lub wartości 169

Etykiety 169

Budowanie grafu gospodarzy za pomocą Neo4j 169

Eksploracja przeglądarki Neo4j 175

Tworzenie i kwerendowanie informacji 176

Tworzenie węzła 177

Pobieranie węzła 178

Tworzenie relacji między węzłami 181

Indeksowanie w celu zwiększenia wydajności 182

Usuwanie obiektu 184

Alternatywne sposoby kwerendowania grafowych baz danych 184

Podsumowanie 185

Pytania 185

Rozdział 6. Budowanie kompleksowego grafu wiedzy 187

Wymagania techniczne 188

Studium przypadku - fikcyjna korporacja Shadow Bunny 188

Pracownicy i zasoby 189

Budowanie grafu 190

Tworzenie węzłów komputerów 193

Dodawanie relacji, aby wskazać administratorów maszyn 194

Konfigurowanie edytora zapytań, aby umożliwił wykonywanie zapytań składających się z wielu instrukcji 196

Mapowanie chmury! 201

Importowanie zasobów chmurowych 204

Tworzenie użytkownika IAM usługi AWS 204

Wykorzystanie narzędzi klienckich AWS do eksportowania danych 209

Ładowanie danych CSV do grafowej bazy danych 215

Ładowanie danych CSV oraz tworzenie węzłów i relacji 216

Grupowanie danych 219

Dodawanie większej ilości danych do grafu wiedzy 220

Active Directory 221

Zespół niebieski i źródła danych IT 221

Zasoby w chmurze 222

OSINT, dane wywiadowcze o zagrożeniach i informacje o lukach w zabezpieczeniach 222

Książki adresowe i wewnętrzne systemy katalogowe 223

Odkrywanie nieznanego i skanowanie portów 223

Rozszerzać istniejący graf czy budować go od podstaw? 223

Podsumowanie 224

Pytania 224

Rozdział 7. Polowanie na poświadczenia 225

Wymagania techniczne 226

Sposoby szukania poświadczeń w postaci zwykłego tekstu 226

Poszukiwanie typowych wzorców w celu identyfikacji poświadczeń 227

Przeszukiwanie dokumentów pakietu Microsoft Office 233

Wydobywanie zapisanych haseł sieci Wi-Fi w systemach Windows 235

Narzędzia do zautomatyzowanego wykrywania poświadczeń 238

Wykorzystanie technik indeksowania do wyszukiwania poświadczeń 239

Używanie narzędzia Sourcegraph do efektywniejszego znajdowania sekretów 239

Wyszukiwanie poświadczeń przy użyciu indeksowania plików wbudowanego w system operacyjny 246

Indeksowanie kodu i dokumentów przy użyciu frameworku Apache Lucene i modułu Scour 252

Polowanie na teksty zaszyfrowane i skróty 254

Polowanie na teksty zaszyfrowane 254

Polowanie na skróty 254

Podsumowanie 262

Pytania 262

Rozdział 8. Zaawansowane polowanie na poświadczenia 263

Wymagania techniczne 264

Metoda pass-the-cookie 264

Poświadczenia w pamięci procesów 266

Korzystanie z narzędzia ProcDump w systemie Windows 266

Mimikittenz 269

Zrzucanie pamięci procesów w systemie Linux 270

| | |
|--|-----|
| Debugowanie procesów i pivotowanie w systemie macOS przy użyciu LLDB | 273 |
| Korzystanie z narzędzia Mimikatz w trybie offline | 275 |
| Śledzenie dostawcy WinINet | 277 |
| Deszyfrowanie ruchu TLS za pomocą rejestrowania kluczy TLS | 282 |
| Przeszukiwanie plików dzienników pod kątem poświadczeń i tokenów dostępu | 288 |
| Wyszukiwanie poufnych informacji w argumentach wiersza poleceń | 293 |
| Przeglądanie argumentów wiersza poleceń w systemach Windows przy użyciu Menedżera zadań oraz WMI | 294 |
| Menedżer poświadczeń systemu Windows i Pęk kluczy systemu macOS | 296 |
| Korzystanie z Menedżera poświadczeń systemu Windows | 297 |
| Pęk kluczy systemu macOS | 301 |
| Korzystanie z optycznego rozpoznawania znaków do wyszukiwania poufnych informacji na obrazach | 302 |
| Eksploatacja domyślnych poświadczeń lokalnych kont administratorów | 305 |
| Ataki phishingowe i spoofing monitów o poświadczenia | 305 |
| Wykorzystanie narzędzia osascript do spoofingu monitu o poświadczenia w systemie macOS | 306 |
| Wykorzystanie narzędzia zenity do spoofingu monitu o poświadczenia w systemie Linux | 307 |
| Wykorzystanie narzędzia PowerShell do spoofingu monitu o poświadczenia w systemie Windows | 309 |
| Wykorzystanie języków JavaScript i HTML do spoofingu okna dialogowego poświadczeń w przeglądarce | 310 |
| Używanie przezroczystych przekaźnikowych serwerów proxy do przeprowadzania ataków phishingowych | 310 |
| Wykonywanie ataków typu password spray | 312 |
| Wykorzystanie programu PowerShell do ataków typu password spray | 313 |
| Wykonywanie ataków typu password spray z systemów macOS lub Linux (implementacja bash) | 315 |
| Podsumowanie | 316 |
| Pytania | 317 |
| | |
| Rozdział 9. Wszechstronna automatyzacja | 319 |
| Wymagania techniczne | 319 |
| Automatyzacja COM w systemach Windows | 320 |

| | |
|---|-----|
| Używanie automatyzacji COM do celów ofensywnych testów bezpieczeństwa | 321 |
| Osiąganie celów poprzez automatyzację programów z pakietu Microsoft Office | 326 |
| Automatyzacja wysyłania e-maili za pośrednictwem programu Outlook | 326 |
| Automatyzacja programu Microsoft Excel za pomocą modelu COM | 328 |
| Wykorzystanie automatyzacji COM do przeszukiwania dokumentów pakietu Office | 331 |
| Skrypty programu Windows PowerShell do przeszukiwania dokumentów pakietu office | 333 |
| Automatyzacja i zdalne kontrolowanie przeglądarek internetowych jako technika ataków | 337 |
| Wykorzystanie Internet Explorera podczas posteksploatacji | 338 |
| Automatyzacja i zdalne kontrolowanie przeglądarki Google Chrome | 343 |
| Używanie zdalnego debugowania Chrome do szpiegowania użytkowników | 348 |
| Wykorzystanie Selenium do automatyzacji przeglądarek | 353 |
| Eksfiltrowanie informacji za pośrednictwem przeglądarki | 363 |
| Podsumowanie | 363 |
| Pytania | 364 |
| | |
| Rozdział 10. Ochrona pentestera | 365 |
| Wymagania techniczne | 366 |
| Blokowanie maszyn (tarcze w górę) | 366 |
| Ograniczenie powierzchni ataku w systemie Windows | 367 |
| Tryb utajony i ograniczanie powierzchni ataku w systemie macOS | 370 |
| Konfigurowanie nieskomplikowanego firewalla (UFW) w systemie Ubuntu | 378 |
| Blokowanie dostępu przez SSH | 380 |
| Zagrożenia komunikacji Bluetooth | 381 |
| Pilnowanie kont administratorów maszyn | 381 |
| Wykorzystanie niestandardowego pliku hostów do przekierowywania niechcianego ruchu do śmieci | 383 |
| Zachowywanie prywatności podczas wykorzystywania do pracy aplikacji typu Office Delve, G Suite czy Facebook | 384 |
| Bezpieczne usuwanie plików i szyfrowanie dysków twardych | 384 |
| Ulepszanie dokumentacji za pomocą niestandardowych znaków zachęty powłoki hakera | 385 |
| Dostosowywanie znaków zachęty powłoki Bash | 385 |
| Dostosowywanie znaków zachęty programu PowerShell | 386 |

| | |
|---|-----|
| Dostosowywanie znaków zachęty programu cmd.exe | 387 |
| Automatyczne rejestrowanie poleceń | 387 |
| Korzystanie z multiplekserów terminalowych i odkrywanie alternatywnych powłok | 388 |
| Monitorowanie logowań i prób logowania oraz wysyłanie alertów | 391 |
| Wykorzystanie mechanizmu PAM do otrzymywania powiadomień związanych z logowaniem się w systemie Linux | 392 |
| Alerty o logowaniach w systemie macOS | 400 |
| Alerty o logowaniach w systemie Windows | 400 |
| Podsumowanie | 406 |
| Pytania | 406 |
| | |
| Rozdział 11. Pułapki, podstępny i honeypoty | 407 |
| Wymagania techniczne | 408 |
| Aktywna obrona zasobów pentestowych | 408 |
| Korzystanie z audytowych list ACL systemu Windows | 409 |
| Użycie list SACL do skonfigurowania pliku do audytowania przez system Windows | 409 |
| Wyzwalanie zdarzenia inspekcji i zmiana zasad inspekcji systemu Windows | 413 |
| Powiadomienia dla zdarzeń inspekcji pliku w systemie Windows | 416 |
| Wysyłanie powiadomień pocztą elektroniczną w systemie Windows | 419 |
| Tworzenie zaplanowanego zadania w celu uruchomienia monitora strażnika | 421 |
| Budowanie strażnika gospodarzy, czyli podstawowej usługi systemu Windows do ochrony hostów | 424 |
| Instalowanie programu Visual Studio Community Edition i tworzenie szablonu usługi systemu Windows | 425 |
| Dodanie do szkieletu podstawowej funkcjonalności | 426 |
| Dodanie do usługi funkcjonalności logowania | 430 |
| Wykorzystanie pliku konfiguracyjnego w celu dostosowania ustawień | 431 |
| Dodanie instalatora do usługi | 431 |
| Usuwanie instalacji usługi Homefield Sentinel | 435 |
| Monitorowanie dostępu do plików honeypotów w systemie Linux | 437 |
| Tworzenie pliku klucza RSA honeypota | 437 |

Używanie narzędzia inotifywait do uzyskiwania podstawowych informacji o dostępie do pliku 438

Wykorzystanie narzędzia auditd do ochrony maszyn pentestowych 439

Powiadomienia wykorzystujące dyspozytor zdarzeń i niestandardowe rozszerzenia narzędzia audisp 444

Alarmowanie o podejrzanym dostępie do plików w systemie macOS 446

Wykorzystanie narzędzia fs_usage do szybkiego i prostego monitorowania dostępu do plików 446

Tworzenie zadania demona LaunchDaemon do monitorowania dostępu do plików wabika 447

Obserwowanie strumienia zdarzeń audytowych OpenBSM 449

Konfigurowanie OpenBSM do inspekcji dostępu w celach odczytu plików wabików 450

Podsumowanie 453

Pytania 454

Rozdział 12. Taktyki zespołu niebieskiego stosowane wobec zespołu czerwonego 455

Scentralizowane rozwiązania monitorowania wykorzystywane przez zespoły niebieskie 456

Korzystanie z osquery w celu pozyskiwania informacji i ochrony zasobów pentestowych 457

Instalowanie oprogramowania osquery na Ubuntu 458

Podstawy obsługi osquery 459

Używanie osquery do monitorowania dostępu do plików wabików 464

Wykorzystanie narzędzi Filebeat, Elasticsearch i Kibana 467

Uruchamianie systemu Elasticsearch przy użyciu Dockera 468

Instalowanie narzędzia Kibana do analizy plików dzienników 471

Konfigurowanie narzędzia Filebeat do wysyłania dzienników do Elasticsearch 472

Ostrzeganie za pomocą Watchera 477

Podsumowanie 478

Pytania 478

Dodatek A. Odpowiedzi 479