

Spis treści

Wstęp	23
<i>Michał Sajdak</i>	
O etyce w hackingu	27
<i>Gynvael Coldwind</i>	
Wstęp	29
Ogólne zasady etycznego hackingu	31
Prawa drugiej strony	31
Radioaktywne dane	32
Prawdziwi ludzie	36
Wprowadzanie podatności	37
Hacking a jurysdykcja i prawo	39
Szukanie błędów	41
Błędy w oprogramowaniu uruchamianym lokalnie	42
Analiza oprogramowania	44
Publikacja podatności	46
<i>Full Disclosure</i>	47
<i>Coordinated Vulnerability Disclosure</i>	49
<i>n-day Policy</i>	50
Udostępnione informacje	51
Błędy i pieniądze	52
Jak szybko zgłaszać błędy?	54
W jakich sytuacjach nie zgłaszać błędów?	56
Błędy w cudzych serwisach, sieciach i systemach	57
Przypadkowe znalezienie błędu	59
<i>Bug bounty</i> , regulaminy i nagrody	61
Zostać bughunterem	62
Ciemna strona <i>bug bounty</i>	65
Trenowanie bez obaw	66
Ogólne wskazówki	66
Wybrane specjalizacje	68
Inżynieria wsteczna	68
Analiza złośliwego oprogramowania	69
Informatyka śledcza	71
Testy penetracyjne i im podobne	72
Powodzenia!	73
Dalsze poszerzanie wiedzy	73

Co każdy administrator powinien wiedzieć o bezpieczeństwie aplikacji webowych	77
<i>Michał Sajdak</i>	
Wstęp	79
Żelazne podstawy protokołu HTTP	80
RCE, czyli w jaki sposób hackerzy hackują serwery (korzystając z aplikacji webowych)	85
Problemy z uwierzytelnianiem	94
Lokalne usługi vs aplikacje webowe	98
Uprawnienia w systemie plików	100
Aplikacja webowa w środowisku testowym oraz wdrożenie na produkcję	101
Problemy z panelami webowymi urządzeń sieciowych	103
Problemy bezpieczeństwa z mechanizmami API	107
Mity związane z bezpieczeństwem aplikacji webowych	112
Kto jest odpowiedzialny za bezpieczeństwo aplikacji webowych?	115
Podsumowanie	116
Dalsze poszerzanie wiedzy	116
Android – bezpieczeństwo systemu i podstawy testów penetracyjnych aplikacji mobilnych	121
<i>Marek Rzepecki</i>	
Wstęp	123
Bezpieczeństwo systemu Android	124
Podstawowa architektura systemu Android	125
Krok pierwszy: Boot ROM	125
Krok drugi: Bootloader	125
Krok trzeci: wczytanie jądra systemu (Kernel)	126
Krok czwarty: rozpoczęcie procesu (Init Process)	127
Krok piąty: zygota (Zygote)	128
Krok szósty: serwer systemowy (System Server)	128
Maszyna wirtualna i kompilacja aplikacji	129
Mechanizmy bezpieczeństwa w systemie Android	130
Chain of trust	130
Przydzielanie uprawnień: SELinux	131
Izolacja aplikacji: sandboxing	133
Szyfrowanie danych	134
Full Disk Encryption (FDE)	135
File Based Encryption (FBE)	135
Zaufane środowisko wykonawcze (Trusted Execution Environment, TEE)	136
Zwiększenie uprawnień (rootowanie)	137
Konsekwencje posiadania uprawnień root	138
Uprawnienia aplikacji w systemie	139
W jaki sposób smartfony są infekowane z użyciem złośliwego oprogramowania	139
Google Play Protect	143
Bezpieczeństwo aplikacji mobilnych na platformę Android	144
Przygotowanie środowiska	144
Inne narzędzia z Android SDK, które warto znać	147
Apksigner	147
Android Asset Packaging Tool (AAPT2)	147
Rootowanie urządzenia	147

Statyczna analiza bezpieczeństwa aplikacji	148
Odzyskiwanie pakietu .apk aplikacji	149
Podstawy analizy statycznej aplikacji	151
Plik AndroidManifest.xml	151
Plik Classes.dex	152
Ważne foldery aplikacji zainstalowanej na smartfonie	152
Inżynieria wsteczna aplikacji i odzyskiwanie kodu źródłowego	153
Przegląd plików aplikacji w kontekście bezpieczeństwa	155
Zbieranie informacji z pliku AndroidManifest.xml	156
Komunikacja pomiędzy aplikacjami	156
Automatyzacja rekonesansu	160
Analiza dynamiczna aplikacji mobilnej	161
Narzędzia do dynamicznej analizy bezpieczeństwa aplikacji	161
Frida	162
Objection	165
Drozer	169
Typowe zabezpieczenia aplikacji mobilnych oraz sposoby ich omijania	171
Antyroot	171
Przesyłanie ruchu sieciowego aplikacji mobilnej przez proxy	173
Pinning certyfikatów	176
Zaciemnienie kodu	178
Mechanizmy aplikacji mobilnych, w których warto szukać błędów	179
WebView	179
Podatności w komponentach aplikacji i schematach URL	184
Podsumowanie	192
Dalsze poszerzanie wiedzy	192
iOS – bezpieczeństwo systemu i podstawy testów penetracyjnych aplikacji mobilnych	199
<i>Marek Rzepecki</i>	
Wstęp	201
Bezpieczeństwo systemu iOS	203
Podstawowa architektura systemu iOS, czyli co się dzieje po uruchomieniu urządzenia	203
Boot ROM	204
iBoot	204
iOS	204
Secure Enclave	204
Mechanizmy bezpieczeństwa w systemie iOS	206
Secure Boot	206
Sandboxing	206
Klasy ochrony danych	208
Keychain	210
Dodatkowe mechanizmy zabezpieczające urządzenie i dane użytkownika	212
Jailbreak, czyli ucieczka z więzienia	216
Konsekwencje wykonania jailbreaka	217
Bezpieczeństwo aplikacji mobilnych na platformę iOS	218
Przygotowanie środowiska	219
Jailbreak	219
Przydatne moduły Cydii	220
OpenSSH	220

Filza File Manager	221
Clutch	222
AppSync Unified	223
Xcode	223
Tworzenie profilu dewelopera	223
Instalacja podpisanej aplikacji	224
Wyświetlanie logów urządzenia	225
Podstawy budowy aplikacji: pasywny rekonesans	225
Odzyskanie pakietu .ipa aplikacji	226
Struktura pliku aplikacji: podstawowy rekonesans	228
Jak odzyskać kod źródłowy aplikacji?	230
Automatyzacja analizy statycznej	231
Analiza dynamiczna bezpieczeństwa aplikacji	232
Narzędzia	232
Frida	232
Grapefruit	236
Objection	237
Typowe zabezpieczenia aplikacji mobilnych oraz sposoby na ich omijanie	242
Anty jailbreak	242
Przesyłanie ruchu sieciowego aplikacji mobilnej przez proxy	246
Pinning certyfikatów	248
Zaciemnienie (obfuskacja) kodu	250
Mechanizmy aplikacji mobilnych, w których warto szukać błędów	252
WebView	252
Komunikacja pomiędzy aplikacjami: schematy URL	257
Podsumowanie	259
Dalsze poszerzanie wiedzy	259

Testy penetracyjne 265

Marcin Piosek

Wstęp	267
Podstawowe pojęcia	267
Motywacja	268
Zakres prac	270
Elementy, które mają zostać poddane audytowi	270
Socjotechnika w testach penetracyjnych	272
Red teaming a testy penetracyjne	272
Bug bounty a testy penetracyjne	274
Decyzja	275
Metodyki i standardy	276
Testy manualne i automatyczne	277
Certyfikaty	278
Proces realizacji zewnętrznych testów bezpieczeństwa	279
Rozmowa z wykonawcą	279
Pytania o zakres testu	280
Oferta i kwestie formalne	282
Którą skrzynkę wybrać?	283
Przygotowanie	283
Wykonanie testów	285

Raport	285
Retest	286
Odbiór prac	286
Próbujemy własnych sił	288
Szybki skan aplikacji webowej z wykorzystaniem OWASP ZAP	289
Burp Scanner	290
Nessus	292
Jak często przeprowadzać testy penetracyjne	295
Problemy, ryzyka i wątpliwości	296
Ryzyko ogólne	296
Kopie zapasowe	297
Środowisko testowe a środowisko produkcyjne	297
Środowisko nie do końca testowe	298
Coś nie działa	299
Aktywne osłony typu Web Application Firewall	299
Testy infrastruktury a tunel VPN	299
Kopiuj i wklej	300
Higiena	300
Gwarancje	301
Niska wycena	301
Podsumowanie	301
Dalsze poszerzanie wiedzy	302

Wprowadzenie do Cyber Threat Intelligence 305

Bartosz Jerzman

Wstęp	307
Czym jest Cyber Threat Intelligence?	307
Intelligence w CTI	308
Geneza CTI	311
Typy aktorów	313
Aktorzy państwowi	313
Aktorzy związani z przestępczością kryminalną	313
Haktywiści	314
Nazwy aktorów	314
Modele stosowane w CTI	314
Cyber Kill Chain®, łańcuch ataku	315
Diamond Model, model diamentowy	317
MITRE ATT&CK® i Attack Flow	319
Kto i dlaczego potrzebuje Cyber Threat Intelligence?	321
Wsparcie CTI dla zespołu reagowania na incydenty komputerowe (SOC/CSIRT)	321
Wsparcie CTI dla DFIR	322
Wsparcie CTI dla <i>threat hunting</i>	322
Wsparcie CTI dla <i>red team/purple team</i>	323
Wsparcie CTI dla architektów i administracji IT	323
Wsparcie CTI w obszarze zarządzania podatnościami (<i>vulnerability management</i>)	323
Wsparcie CTI w obszarze zarządzania ryzykiem i bezpieczeństwem	324
Czym nie jest Cyber Threat Intelligence	324
Produkty Cyber Threat Intelligence	325
Raporty taktyczne	325

Raporty operacyjne	326
Raporty strategiczne	326
Produkty techniczne	326
Budowa zespołu Cyber Threat Intelligence	327
Dla zarządzających bezpieczeństwem w organizacji	327
Budżet	328
Model dojrzałości CTI	328
Umiejscowienie CTI w strukturze organizacji	329
Dla szefów zespołu CTI	329
Wymagania i priorytety	329
Portfolio produktów	330
Ludzie i struktura	331
Źródła	333
Narzędzia	333
Dla analityków CTI	334
Profilowanie zagrożeń	335
Jakie elementy powinien zawierać profil aktora/grupy?	337
Podstawowy opis	337
Wiktymologia	337
Infrastruktura	337
Taktyka	338
Narzędzia i malware	338
TTP (taktyki, techniki, procedury)	338
Historia operacji	339
Przykłady profili	339
Profile zagrożeń oparte na ustrukturyzowanych modelach danych	340
Praktyczna analiza CTI (poziom taktyczny)	341
Modelowanie danych	342
Wzbogacanie danych - <i>pivoting</i>	345
Klastrowanie	347
Aktywne śledzenie grup i klastrów zagrożeń	351
Podsumowanie	352
Dalsze poszerzanie wiedzy	352

Modelowanie zagrożeń i analiza ryzyka aplikacji **357**

Lukasz Basa, Wiktor Sędkowski

Wstęp	359
Co to jest modelowanie zagrożeń i dlaczego trzeba je przeprowadzić?	359
Podstawowe pojęcia	360
Modelowanie zagrożeń	361
Niezbędne zasoby	361
Identyfikacja komponentów	362
Zaangażuj w proces odpowiednie osoby	363
Zrozum swoją aplikację	363
Diagramy	365
Diagramy przepływu danych	365
Diagramy przepływu procesów	366
Diagramy sekwencji	368

Diagramy czynności	370
Który rodzaj diagramów jest odpowiedni dla konkretnego użytkownika?	371
Weryfikacja diagramów	371
Poznaj swojego wroga	372
Ustrukturyzowane podejście do modelowania	373
STRIDE	373
NIST 800-154	375
PASTA	376
VAST	378
TRIKE	379
LINDDUN	380
Frameworki wspierające identyfikację zagrożeń	383
OWASP Top Ten	383
MITRE ATT&CK® Framework	385
Cyber Threat Framework	386
CWE	387
CAPEC	388
CVSS	388
Drzewa ataku	390
Cyber Kill Chain®	393
Fazy ataku	393
Wady CKC	396
Praktyczne wdrożenie modelu	396
Narzędzia	398
Narzędzia biurowe	398
CAIRIS	399
OWASP Threat Dragon	401
IriusRisk	402
Microsoft TMT	404
ThreatModeler	406
Elevation of Privilege	407
STIX	409
Modelowanie kodem	411
Automatyzacja procesu modelowania zagrożeń	411
Modelowanie z threatspec	412
Threagile dla DevOps	414
Analiza ryzyka	415
Podejście jakościowe	418
Podejście ilościowe	419
Postępowanie z ryzykiem	421
Kryteria akceptacji ryzyka	421
Podsumowanie	422
Dalsze poszerzanie wiedzy	423
Wprowadzenie do frameworka MITRE ATT&CK®	427
Wojciech Lesicki	
Wstęp	429
ATT&CK®, czyli...	429
Co kryje opis danej techniki?	431

Nawigator – skuteczna pomoc	432
ATT&CK a Cyber Threat Intelligence	434
ATT&CK dla hunterów	439
Od jakich technik warto zacząć przegląd?	439
Threat hunting a źródła danych	442
ATT&CK dla atakujących	447
Podsumowanie	456
Dalsze poszerzanie wiedzy	457

Kryptologia z lotu ptaka **461**

Iwona Polak

Wstęp	463
Definicja podstawowych pojęć	464
Cechy dobrego szyfru	464
Szyfrowanie i deszyfrowanie	465
Co nie jest szyfrowaniem	466
Szyfrowanie vs kodowanie	466
Kryptografia vs steganografia	467
Szyfry klasyczne	468
Szyfry współczesne	470
Szyfry blokowe	470
Dopełnienie (<i>padding</i>)	471
Tryby szyfrów blokowych	472
Szyfry strumieniowe	474
Szyfr z kluczem jednorazowym (OTP)	475
Szyfry asymetryczne	477
Szyfrowanie hybrydowe	478
Skąd się biorą szyfry?	480
Szyfry blokowe	480
Szyfry strumieniowe	482
Szyfry asymetryczne	483
Kryptoanaliza	483
Funkcje skrótu	485
Kody HMAC	490
Podpisy cyfrowe	490
Zastosowania	494
Podpisywanie tokenów JWT	494
Uwierzytelnienie za pomocą klucza w protokole SSH	496
Protokół TLS	498
Korzystaj z gotowych rozwiązań	499
Dalsze poszerzanie wiedzy	502

Wprowadzenie do bezpieczeństwa przemysłowych systemów sterowania (ICS/OT) **509**

Marcin Dudek

Wstęp	511
O czym mówimy	512
Dlaczego to ważne	512
Elementy przemysłowe i słownictwo	513

ICS, OT czy IACS	513
Systemy SCADA i DCS	515
Panele HMI	516
Sterowniki PLC	516
Stacje inżynierskie (EWS)	519
Historian	520
Systemy SIS	520
Z historii ataków	521
Stuxnet (2009)	522
BlackEnergy (2015)	523
Industroyer/Crashoverride (2016)	526
Triton/Trisis (2017)	529
Ataki oportunistyczne i ransomware'owe	531
Wnioski z ataków	533
Budowa własnego środowiska laboratoryjnego	535
Bezpieczeństwo elementów przemysłowych	540
Protokoły przemysłowe	541
Protokół przemysłowy Modbus jako przykład	542
Ćwiczenia z Modbusem	545
Skanowanie sieci	545
Odczyt danych ze sterownika	547
Zapis na sterownik	549
Analiza ruchu sieciowego	550
Sterowniki PLC	552
Bezpieczeństwo logiki	552
Bezpieczna konfiguracja	552
Bezpieczeństwo usług	553
Błędy w oprogramowaniu wbudowanym (firmware)	554
Protokoły administracyjne – ćwiczenie	554
Podstawy bezpiecznej architektury	556
Segmentacja	556
Komunikacja OT z sieciami zewnętrznymi	559
Najważniejsze punkty architektury	560
Podsumowanie: IT vs OT	561
Dalsze poszerzanie wiedzy	563
Bezpieczeństwo danych w spoczynku – szyfrowanie i usuwanie danych	569
<i>Krzysztof Wośński</i>	
Wstęp	571
Czy szyfrowanie jest zawsze skuteczne?	572
Jak działa szyfrowanie	576
Szyfrowanie danych w spoczynku	579
Szyfrowanie a RODO	579
Moduł TPM	580
Dyski samoszyfrujące – SED	582
Pełne szyfrowanie dysku – FDE	584
Windows – BitLocker	585
macOS – FileVault	590
Linux	591

Szyfrowanie dysków przy użyciu oprogramowania VeraCrypt	593
File-Based Encryption (FBE)	595
Szyfrowanie w smartfonach	595
Oprogramowanie VeraCrypt	596
Inne rodzaje oprogramowania do szyfrowania plików	596
Standardy zabezpieczeń urządzeń przechowujących dane	597
collaborative Protection Profile i Common Criteria	597
FIPS 140-2 i 140-3	598
TCG Opal 2.0	600
Usuwanie danych	600
Usuwanie danych a przenoszenie do kosza i formatowanie	600
Permanentne usuwanie danych z dysków HDD	601
Permanentne usuwanie danych z dysków SSD	603
Windows – kopie w tle	603
Niszczanie i pozbywanie się nośników	605
Niszczanie fizyczne dokumentów i nośników danych	607
Problem zaciemniania danych w sposób warstwowy	609
Usuwanie danych w dokumentach	610
Usuwanie danych ze zdjęć (metadane EXIF)	613
Podsumowanie	614
Dalsze poszerzanie wiedzy	614

OSINT – wprowadzenie 619

Tomasz Turba

Wstęp	621
Cele i sposoby realizacji OSINT-u	624
Przygotowanie do działania	625
Mapa myśli – płaszczyzna ataku	628
Zabezpieczenie anonimowości	628
Przegląd otwartych źródeł	635
Imię i nazwisko, adres e-mail, adres fizyczny	635
Fotografie i metadane	637
Archiwa	639
Infrastruktura	641
Geolokalizacja	643
Dane z deep webu i dark webu	648
Google Hacking Database	651
Narzędzia do pozyskiwania informacji o podmiocie	655
Facebook	656
Twitter	659
LinkedIn	663
Instagram	664
Inne źródła	666
Kombajny do pozyskiwania informacji o organizacji	666
Maltego	667
SpiderFoot	668
theHarvester	669
OSINT a sztuczna inteligencja	670
Zachowania prewencyjne	674

Canarytokens	674
Honeypot	676
Skrócone linki	677
Walka z fake newsami	678
Podsumowanie	681
Dalsze poszerzanie wiedzy	681

Bezpieczeństwo fizyczne – ochrona aktywów 687

Tomasz Dacka

Wstęp	689
Dla kogo jest ten rozdział?	690
Modele zabezpieczeń fizycznych	692
Analiza ryzyka, czyli jak sobie pościelesz, tak się wyśpisz	695
Metoda jakościowa	700
Metoda ilościowa	701
Środki zabezpieczeń fizycznych na przykładzie centrum danych	702
Zabezpieczenia mechaniczne	703
Okna, szklenie	703
Wyrzutnie i czerpnie powietrza	703
Drzwi, zamki	703
Bariery, słupki drogowe	704
Oznakowanie	705
Oświetlenie	706
Elektroniczne systemy bezpieczeństwa (SKD, CCTV, SSWiN, PSIM)	707
Posterunki ochrony fizycznej, element ludzki	710
Architektura elektronicznego systemu ochrony	712
Część pasywna	712
Część aktywna	712
Kamery	713
Systemy kontroli dostępu	714
Centrum nadzoru	715
Security as a service, czyli monitoring wizyjny w chmurze	716
CPTED (Crime Prevention Through Environmental Design)	717
Bezpieczeństwo jako zmienna w czasie	718
Aspekt wdrożeniowy	720
Bezpieczeństwo fizyczne jako ważny czynnik zarządzania ciągłością działania (BCM)	722
Realne przykłady włamań do infrastruktury systemów bezpieczeństwa fizycznego oraz ich konsekwencje	723
Przykład 1: Karta to karta, efekt jest taki sam?	723
Przykład 2: Fizyczne zabezpieczenia punktów styku	723
Przykład 3: Proszę za mną...	723
Przykład 4: Śmieci mają wartość	724
Przykład 5: Przesyłka	724
Przykład 6: Ciemność! Widzę ciemność!	724
Przykład 7: Botnet bezpieczeństwa	724
Przykład 8: Kamera	725
Przykład 9: Ściany mają uszy, bezapelacyjnie	725
Przykład 10: Na szczęście alarm prawdziwy	725
Podsumowanie	726
Dalsze poszerzanie wiedzy	727

Współczesny fuzzing**729**

Marek Zmysłowski

Wstęp	731
Czym jest fuzzing?	731
Zalety fuzzingu	732
Krótką historia fuzzingu	733
Przed AFL-em	733
Nowa era: AFL	734
Zasada działania fuzzerów	734
Rodzaje fuzzingu	736
Sposób generowania danych wejściowych	736
<i>Mutation-based</i>	736
<i>Generation-based</i>	736
Gramatyki	738
Pokrycie kodu aplikacji	738
Fuzzery typu <i>black box</i>	739
Fuzzery wykorzystujące kod źródłowy	739
Fuzzery wykorzystujące kod binarny	740
Sposób restartowania aplikacji	740
Informacja zwrotna	742
Algorytmy genetyczne	742
Instrumentacja	743
Historia	743
Instrumentacja programowa	743
Instrumentacja podczas kompilacji	743
Przebudowywanie aplikacji	744
Instrumentacja dynamiczna	744
Wirtualizacja i emulacja	745
Instrumentacja sprzętowa	745
Sanitizery	746
Fuzzowanie a systemy operacyjne	748
AFL++	748
WinAFL	754
Fuzzer wtf	754
LibAFL	754
honggfuzz	754
ClusterFuzz	757
Centipede	757
Nyx	757
Wykonanie symboliczne	757
<i>Concolic execution</i>	758
Fuzzing przeglądarek internetowych	759
Podsumowanie	760
Dalsze poszerzanie wiedzy	760

Mechanizmy uwierzytelniania wiadomości e-mail – SPF, DKIM i DMARC 763

Grzegorz Trawiński

Wstęp	765
Sender Policy Framework (SPF)	765
Możliwe wartości SPF	767
SPF – testy	772
Marketing Automation as a Service	776
SPF i bug bounty	777
DomainKeys Identified Mail (DKIM)	777
DKIM – testy	779
DKIM – niezaprzeczalność	782
DKIM – bug bounty	782
Mail.From vs From	783
Domain-based Message Authentication, Reporting, and Conformance (DMARC)	784
DMARC – p=none	788
DMARC – raportowanie	788
DMARC – testy	789
DMARC – bug bounty	791
Czy mechanizmy SPF, DKIM i DMARC chronią przed phishingiem?	791
Nowy obowiązek związany z obsługą poczty e-mail	793
Zmiana w polskim prawie	793
Projekt: bezpiecznapoczta.cert.pl	793
Podsumowanie	793
Dalsze poszerzanie wiedzy	795

hashcat – wyścig w funkcji sił i środków 799

Konrad Jędrzejczyk

Wstęp	801
Podstawowe pojęcia	801
Właściwości funkcji skrótu	804
Zastosowanie funkcji skrótu	806
Sól i pieprz	806
Czym jest hashcat	807
Hashołamacz, czyli budujemy maszynę do łamania hashy	808
Wybór lokalizacji dla maszyny	808
Zasilanie	808
Procesor i pamięć	809
Płyta główna	809
Dysk twardy	809
System operacyjny	810
Dobór kart graficznych	811
Instalacja hashcata	815
Windows	815
Linux	816
Chmura, czyli grad kosztów	817
Hashtopolis, czyli stos komputerów i korporacyjna kolejka	819
Opracowanie taktyki ataku z wykorzystaniem hashcata	821
Pozyskiwanie hashy	821

Identyfikacja hashy	822
Rekonesans	823
Tryby ataku	824
Atak słownikowy	824
Atak kombinacyjny	828
Atak przy użyciu maski	828
Atak hybrydowy	830
Moduł brain	831
Jak tworzyć hasła?	832
Mnemotechnika	833
Co robić, jak żyć?	834
Menedżer haseł	834
Podsumowanie	835
Dalsze poszerzanie wiedzy	836

Wprowadzenie do narzędzia Metasploit 841

Piotr Ptaszek

Wstęp	843
Wprowadzenie	843
Czym jest Metasploit?	843
MSFconsole	844
Konfiguracja Metasploita w systemach Ubuntu oraz Windows	845
Instalacja w systemie Ubuntu	845
Praca z Metasploitem	846
Exploits	847
Payloads	847
Auxiliary	848
Options	849
Set i Unset	849
Info i Help	850
Zbieranie informacji o usługach	851
Eksploity	853
Importowanie exploitów	854
msfvenom	856
Czym jest msfvenom?	856
Tworzenie ładunku	856
Kodowanie ładunków	857
Armitage	858
Nmap w Metasploicie	860
Podstawy narzędzia Nmap	860
Nmap we współpracy z bazą danych narzędzia Metasploit	862
Obszar roboczy	864
Meterpreter i eksploitacja powłamańowa	865
Podstawowe komendy	865
mimikatz/Kiwi	870
Instalacja środowiska testowego Metasploitable3 w VirtualBox	872
Czym jest Metasploitable?	872
Tworzenie sieci NAT	873

Przykładowa eksploatacja środowiska testowego Metasploitable3	874
Zbieranie informacji	874
Eksploatacja środowiska Ubuntu 14.04	875
Eksploatacja środowiska Windows Server 2008 R2	876
Faza poeksploatacyjna	878
Podsumowanie	881
Dalsze poszerzanie wiedzy	881

PowerShell w ofensywie **883**

Paweł Maziarz

Wprowadzenie	885
Rekonesans	887
Pobranie interesujących wpisów DNS dla danej domeny	888
Enumeracja odwrotnych adresów DNS (reverse DNS)	889
Enumeracja jednoliterowych poddomen	890
Enumeracja poddomen z wykorzystaniem słownika	891
Wyszukiwanie poddomen na podstawie rejestrowanych certyfikatów SSL	893
Skaner wirtualnych hostów WWW	894
Skaner portów TCP	895
Skaner portów TCP i banerów	896
Skaner wersji serwerów HTTP	897
Uzbrojenie	899
Pobranie i uruchomienie skryptu po HTTP/HTTPS	899
Pobranie i uruchomienie skryptu po HTTP/HTTPS ukrytego w nagłówku odpowiedzi 404	900
Pobranie i uruchomienie skryptu zapytaniem DNS	900
Pobranie i uruchomienie zapytaniem DNS skryptu zakodowanego w Base64	901
Pobranie i uruchomienie zapytaniem DNS wielolinijkowego skryptu zakodowanego w Base64	901
Pobranie i uruchomienie skryptu z wykorzystaniem DNS-over-HTTPS (DoH)	902
Zakodowanie do Base64 polecenia do uruchomienia przez PowerShella	903
Stworzenie skrótu (plik .lnk) uruchamiającego złośliwe polecenie PowerShella	904
Przygotowanie wykonywalnego pliku .exe uruchamiającego skrypt PowerShella	904
Kompilacja programu w języku C# do wykonywalnego pliku .exe za pomocą PowerShella	905
Dostarczenie	906
Wysłanie pliku poprzez formularz WWW	906
Wysłanie pliku na serwer FTP	907
Wysłanie wiadomości e-mail z wykorzystaniem wskazanego serwera SMTP	907
Wysłanie e-maila ze skonfigurowanego Microsoft Outlooka	908
Eksploatacja	908
Pobranie i uruchomienie docelowego złośliwego oprogramowania z uprawnieniami administratora	908
Ominięcie polityki uruchamiania skryptów	910
Uruchomienie polecenia w systemie operacyjnym za pomocą Microsoft SQL Server	912
Kradzież haseł użytkownika	914
Próba łamania haseł innych użytkowników	915
Instalacja	917
Uruchomienie skryptu po zalogowaniu – klucze Run/RunOnce w rejestrze	917
Uruchomienie skryptu po zalogowaniu – folder Startup	919
Malware jako komenda do debugowania aplikacji	919
Malware jako komenda do debugowania cichego zakończenia programu	920
Uruchom kod PowerShella jako zaplanowaną pracę	921

Uruchom kod PowerShella jako zaplanowane zadanie	921
Usługa Windows uruchamiająca kod PowerShella	922
<i>Command and control</i>	923
Komunikacja po HTTP/HTTPS	923
Serwer HTTP	924
Komunikacja z wykorzystaniem serwera FTP	927
Bezpośrednie połączenie TCP	930
Komunikacja po DNS	932
Komunikacja po DNS-over-HTTPS	936
Cele misji	936
Odnalezienie serwerów Microsoft SQL	937
Eksfiltracja po ICMP	938
Eksfiltracja danych z wykorzystaniem Outlooka	940
Wyczyszczenie logów	941
Podsumowanie	942
Dalsze poszerzanie wiedzy	942