

Spis treści

PODZIĘKOWANIA	11
WPROWADZENIE	12
CZĘŚĆ I. PODSTAWY	15
1	
CZYM JEST INŻYNIERIA SPOŁECZNA	17
Ważne pojęcia w inżynierii społecznej	18
Atak pod pretekstem	18
Biały wywiad	18
Phishing	19
Spearphishing	19
Whaling	20
Vishing	20
Przynęta	21
Nurkowanie po śmietnikach	22
Koncepcje psychologiczne w inżynierii społecznej	22
Wpływ	23
Manipulacja	23
Porozumienie	23
Sześć zasad perswazji według dr. Cialdiniego	23
Współczucie a empatia	26
Podsumowanie	27
2	
WZGLĘDY ETYCZNE W INŻYNIERII SPOŁECZNEJ	28
Etyczna inżynieria społeczna	29
Ustalanie granic	29
Zrozumienie uwarunkowań prawnych	30
Zrozumienie uwarunkowań korzystania z usług	30
Raport po akcji	31

Studium przypadku: inżynieria społeczna posunięta za daleko	31
Etyczne zbieranie danych OSINT-owych	32
Ochrona danych	32
Przestrzeganie prawa i przepisów	34
Studium przypadku: granice etyczne inżynierii społecznej	35
Podsumowanie	37

CZĘŚĆ II. OFENSYWNA INŻYNIERIA SPOŁECZNA 39

3	
PRZYGOTOWANIE DO ATAKU	41
Koordinacja działań z klientem	41
Ustalenie zakresu prac	42
Określenie celów	43
Zdefiniowanie metod	43
Budowanie skutecznych pretekstów	44
Wykorzystanie specjalistycznych systemów operacyjnych w inżynierii społecznej	45
Przestrzeganie kolejności faz ataku	46
Studium przypadku: dlaczego ustalenie zakresu prac ma znaczenie	50
Podsumowanie	50

4	
GROMADZENIE BIZNESOWYCH DANYCH OSINT-OWYCH	51
Studium przypadku: dlaczego OSINT ma znaczenie	52
Zrozumienie rodzajów działań OSINT-owych	52
OSINT biznesowy	53
Pozyskiwanie podstawowych informacji biznesowych z Crunchbase	53
Identyfikacja właścicieli stron internetowych za pomocą WHOIS	57
Zbieranie danych OSINT-owych z użyciem wiersza poleceń za pomocą programu Recon-ng	58
Korzystanie z innych narzędzi: theHarvester i OSINT Framework	66
Znajdowanie adresów e-mail za pomocą Huntera	67
Wykorzystanie narzędzi mapowania i geolokalizacji	67
Podsumowanie	69

5	
MEDIA SPOŁECZNOŚCIOWE I DOKUMENTY PUBLICZNIE DOSTĘPNE	70
Analiza mediów społecznościowych w służbie OSINT-u	71
LinkedIn	71
Strony z ofertami pracy i strony poświęcone karierze zawodowej	74
Facebook	75
Instagram	78
Wykorzystanie wyszukiwarki Shodan do OSINT-u	81
Używanie parametrów wyszukiwania w wyszukiwarce Shodan	82
Wyszukiwanie adresów IP	82
Wyszukiwanie nazw domen	82
Wyszukiwanie nazw hostów i subdomen	83

Automatyczne wykonywanie zrzutów ekranu za pomocą programu Hunchly	84
Myszkowanie po formularzach SEC	86
Podsumowanie	88

6

ZBIERANIE DANYCH OSINT-OWYCH O LUDZIACH	89
Wykorzystanie narzędzi OSINT-owych do analizy adresów e-mail	89
Uzyskanie informacji, czy do systemu użytkownika dokonano włamania za pomocą aplikacji webowej Have I Been Pwned	90
Utworzenie listy kont w mediach społecznościowych za pomocą Sherlocka	91
Tworzenie wykazów kont internetowych za pomocą WhatsMyName	91
Analiza haseł za pomocą Pwdlogy	92
Analiza obrazów Twojego celu	93
Ręczna analiza danych EXIF	94
Analiza obrazów za pomocą ExifTool	95
Analiza mediów społecznościowych bez użycia narzędzi	98
LinkedIn	98
Instagram	99
Facebook	99
Twitter	99
Studium przypadku: kolacja, podczas której ktoś rozdał całe złoto	99
Podsumowanie	101

7

PHISHING	102
Konfiguracja ataku phishingowego	102
Przygotowanie bezpiecznej instancji VPS dla phishingowych stron docelowych	103
Wybór platformy e-mailowej	112
Zakup domen strony wysyłającej i strony docelowej	114
Konfigurowanie serwera webowego phishingu i infrastruktury	115
Dodatkowe kroki w przypadku phishingu	116
Wykorzystanie pikseli śledzących do pomiaru częstotliwości otwierania wiadomości e-mail	116
Automatyzacja phishingu z frameworkiem Gophish	117
Dodanie obsługi HTTPS dla stron docelowych wyłudzających informacje	121
Wykorzystanie skróconych adresów URL w phishingu	123
Wykorzystanie SpoofCard do spoofingu połączeń telefonicznych	123
Czas i sposób przeprowadzenia ataku	123
Studium przypadku: zaawansowany trwały phishing za 25 dolarów	124
Podsumowanie	127

8

KLONOWANIE STRONY DOCELOWEJ	128
Przykład sklonowanej strony internetowej	128
Strona logowania	129
Zakładka z pytaniami wrażliwymi	131

Zakładka informująca o błędzie	132
Pozyskiwanie informacji	133
Klonowanie strony internetowej	134
Odnaalezienie zakładki logowania i zakładki użytkownika	134
Klonowanie zakładek za pomocą HTTrack	135
Zmiana kodu pola logowania	137
Dodawanie zakładek internetowych do serwera Apache	140
Podsumowanie	140

9

WYKRYWANIE, POMIAR I RAPORTOWANIE 141

Wykrywanie	141
Pomiar	142
Wybór wskaźników	143
Odsetek, mediana, średnia i odchylenie standardowe	143
Liczba otwarć wiadomości e-mail	144
Liczba kliknięć	145
Informacje wprowadzane do formularzy	146
Działania podejmowane przez ofiarę	148
Czas wykrycia	148
Terminowość działań korygujących	149
Sukces działań korygujących	149
Ratingi ryzyka	149
Raportowanie	151
Wiedzieć, kiedy wykonać telefon	151
Pisanie raportu	151
Podsumowanie	154

CZĘŚĆ III. OBRONA PRZED SOCJOTECHNIKĄ 155

10

PROAKTYWNE TECHNIKI OBRONY 157

Programy uświadamiające	157
Jak i kiedy szkolić	158
Zasady nienakładania kar	159
Zachęty do dobrego zachowania	160
Przeprowadzanie kampanii phishingowych	160
Monitoring reputacji i OSINT-u	161
Wdrażanie programu monitorowania	161
Outsourcing	162
Reakcja na incydent	162
Proces reagowania na incydenty według instytutu SANS	163
Reakcja na phishing	164
Reakcja na vishing	165
Reakcja na zbieranie danych OSINT-owych	166

Postępowanie z przyciąganiem uwagi mediów	166
Jak użytkownicy powinni zgłaszać incydenty	167
Techniczne środki kontroli i powstrzymanie	167
Podsumowanie	168

11	
TECHNICZNE ŚRODKI KONTROLI POCZTY ELEKTRONICZNEJ	169
Standardy bezpieczeństwa	169
Pola From	170
Poczta identyfikowana kluczami domenowymi (DKIM)	170
Framework polityki nadawcy (SPF)	176
Uwierzytelnianie, raportowanie i zgodność wiadomości w oparciu o domeny	179
Oportunistyczny TLS	182
MTA-STX	183
TLS-RPT	184
Technologie filtrowania poczty elektronicznej	184
Inne zabezpieczenia	185
Podsumowanie	186

12	
TWORZENIE INFORMACJI WYWIADOWCZYCH O ZAGROŻENIACH	187
Korzystanie z Alien Labs OTX	188
Analiza e-maila phishingowego w OTX	189
Tworzenie impulsu	189
Analiza źródła wiadomości e-mail	190
Wprowadzanie wskaźników	191
Testowanie potencjalnie złośliwej domeny w Burp	194
Analiza plików udostępnionych do pobrania	198
Prowadzenie OSINT-u w służbie działań wywiadowczych	199
Przeszukiwanie przy użyciu serwisu VirusTotal	199
Identyfikacja złośliwych stron na podstawie WHOIS	199
Odkrywanie phishów za pomocą platformy PhishTank	201
Przeglądanie informacji za pomocą serwisu ThreatCrowd	202
Konsolidacja informacji w aplikacji webowej ThreatMiner	204
Podsumowanie	205

A	
USTALENIE ZAKRESU PRAC — ARKUSZ ROBOCZY	206

B	
SZABLON RAPORTOWANIA	209
Wprowadzenie	209
Streszczenie wykonawcze	210

Wykaz prac do zrealizowania	210
Ustalenie zakresu prac	210
Data ukończenia pracy	211
Miejsce wykonywania pracy	211
O <Nazwa firmy>	211
Narzędzia i metodologie	211
Wskaźniki	211
Phishing	212
Vishing	212
Odkryte ryzyka	213
Klasyfikacja powagi ryzyka	213
Dyskusja	214
Problem	214
Udowodnienie istnienia problemu	214
Potencjalne wyniki Twojej pracy	214
Łagodzenie skutków lub działania naprawcze	214
Zalecenia	214
Podsumowanie	214
Odkryte numery telefonów	214
Odkryte strony internetowe	214
Odkryte adresy e-mail	215
Odkryte aktywa o wysokiej wartości	215
Wykorzystane preteksty	215

C

ZBIERANIE INFORMACJI — ARKUSZ ROBOCZY	216
--	------------

D

PRÓBKA PRETEKSTU	219
Zdezorientowany pracownik	219
Inwentaryzacja IT	220
Ankieta transparentności	221

E

ĆWICZENIA, KTÓRE POPRAWIAJĄ TWOJĄ SOCJOTECHNIKĘ	222
Pomóż przypadkowej osobie, a następnie poproś o odwzajemnienie przysługi	222
Improwizuj	223
Występ stand-upowy	223
Wystąpienia publiczne/wznoszenie toastów	223
Prowadzenie operacji OSINT-owych na rodzinie i znajomych	224
Rywalizuj w dziedzinie inżynierii społecznej i na OSINT-owych imprezach typu „Zdobądź flagę”	224