

Wstęp.....	3
Rozdział 1: Podstawy Cyberbezpieczeństwa.....	4
Rozdział 2: Kluczowe Pojęcia i Różnice.....	5
2.1 Malware vs. Ransomware vs. Spyware vs. Adware vs. Rootkit.....	5
2.2 Exploit, Payload, Backdoor – co to znaczy?.....	5
2.3 Luka Bezpieczeństwa (Vulnerability) i Exploit.....	6
2.4 Zero-Day – Mit czy Rzeczywistość?.....	6
Rozdział 3: Rodzaje Ataków Hakerskich.....	6
3.1 Phishing, Spear Phishing, Whaling.....	6
3.2 DDoS (Distributed Denial of Service).....	7
3.3 MITM (Man-In-The-Middle).....	7
3.4 Brute Force i Dictionary Attack.....	7
3.5 SQL Injection, XSS, CSRF.....	8
3.6 Social Engineering.....	8
3.7 Ransomware.....	8
Rozdział 4: Narzędzia w Pentestingu.....	9
4.1 Kali Linux i jego zastosowanie.....	9
4.2 Nmap – skanowanie sieci.....	9
4.3 Metasploit – framework do eksploatacji.....	9
4.4 Wireshark – analiza ruchu sieciowego.....	9
4.5 Burp Suite – testowanie aplikacji webowych.....	9
4.6 Aircrack-ng – łamanie sieci Wi-Fi.....	10
4.7 Flipper Zero – multifunkcyjne narzędzie.....	10
Rozdział 5: Etapy Pentestingu.....	10
5.1 Rekonesans (Reconnaissance).....	10
5.2 Skanowanie i analiza (Scanning).....	10
5.3 Eksploatacja (Exploitation).....	11
5.4 Eskalacja uprawnień.....	11
5.5 Utrzymanie dostępu (Persistence).....	11
5.6 Raportowanie i rekomendacje.....	11
Rozdział 6: Ciemna Strona Internetu.....	11
6.1 Dark Web vs. Deep Web – co to jest?.....	11
6.2 Tor i Tails – narzędzia do anonimowości.....	12
6.3 Black Hat, White Hat, Gray Hat – podział hakerów.....	12
6.4 Czym są botnety?.....	12
6.5 Carding i skimming – oszustwa finansowe.....	13
Rozdział 7: Obrona przed Atakami.....	13
7.1 Firewalle i IDS/IPS.....	13
7.2 Antywirusy i EDR.....	13
7.3 Aktualizacje i patch management.....	14
7.4 Kopie zapasowe – offline i online.....	14
7.5 Szyfrowanie danych.....	14
Rozdział 8: Przyszłość Cyberbezpieczeństwa.....	15
8.1 AI i uczenie maszynowe w obronie i ataku.....	15
8.2 Quantum Computing – zagrożenie dla szyfrowania?.....	15
8.3 IoT – internet rzeczy i jego podatności.....	15
Trudne pojęcia:.....	16
Rozdział 9: Słownik pojęć od A do Z i liczby.....	16
Alfabetycznie.....	16
Liczby.....	29
Rozdział 10: Praktyczne Scenariusze.....	30
10.1 Symulowany atak phishingowy – jak wygląda krok po kroku.....	30

10.2 Jak haker łamie hasła – przykład brute force.....	31
10.3 Jak działa ransomware – od infekcji po okup.....	31
Podsumowanie.....	32

## Wstęp

Nazywam się Maciej, ale w środowisku hakerskim znany byłem jako Garret. Być może spotkałeś się kiedyś z tym pseudonimem, może tylko obił Ci się o uszy, a może dopiero teraz go poznajesz. Niezależnie od tego, gdzie się znajdujesz w swojej drodze, chcę zaprosić Cię do wspólnej podróży po świecie pentestingu, hackingu i cyberbezpieczeństwa.

Przyrostek „Thief”, który często pojawia się w mojej nazwie, ma podwójne znaczenie. Po pierwsze, jestem fanem kultowej gry „Thief”, w której wcielamy się w postać Garretta – mistrza skradania i sprytu. Po drugie – muszę być z Tobą szczery – moje pierwsze kroki w cyberprzestrzeni nie zawsze prowadziły mnie ścieżką prawa i etyki. Był czas, gdy działałem na ciemniejszej stronie, niczym wspomniany Garret, poszukujący okazji, by zdobyć to, co ukryte. Jednak z czasem zrozumiałem, że prawdziwa siła i satysfakcja leżą w pomaganiu innym oraz w zabezpieczaniu tego, co wartościowe. Przekułem swoją wiedzę i doświadczenie w firmę zajmującą się cyberbezpieczeństwem – GarretShield – by teraz stawać po jasnej stronie mocy.

Cyberbezpieczeństwo i pentesting to niezwykle fascynująca dziedzina. Pozwala Ci myśleć jak haker, przewidywać zagrożenia, rozpracowywać systemy, znajdować ich słabości – ale wszystko to w celu ich ochrony. To jak gra strategiczna, w której stajesz się obrońcą fortecy, choć czasem musisz myśleć jak napastnik.

Jednak będę z Tobą szczery – ten zawód ma nie tylko blaski, ale i cienie. Ciągła nauka, stres, presja, odpowiedzialność za cudze dane, a czasem samotność, bo niewielu rozumie specyfikę tej pracy. To życie w nieustannym napięciu, w wyścigu z cyberprzestępcami. Ale jeśli masz pasję, ciekawość i odrobinę zdrowego uporu – ten świat może stać się Twoim miejscem.

Ten e-book nie jest encyklopedią z suchymi definicjami. To Twoje pierwsze narzędzie do odkrycia tego świata. Zrozumienie, czym jest ransomware, jak odróżnić malware od spyware, co to jest SQL Injection czy Man-In-The-Middle – to nie tylko puste słowa. To początek Twojej wędrówki ku zostaniu specjalistą, który potrafi rozpoznawać zagrożenia i chronić to, co cenne.

Wyruszmy razem. Gotowy?

# Rozdział 1: Podstawy Cyberbezpieczeństwa

Na samym początku mojej przygody z cyberbezpieczeństwem myślałem, że to głównie praca przy komputerze, kilka linijek kodu i magia dzieje się sama. Nic bardziej mylnego. Szybko odkryłem, że to świat, w którym wiedza jest potęgą, a zrozumienie podstaw stanowi fundament każdego sukcesu. Chcę Ci przekazać tę lekcję już teraz, na starcie.

Cyberbezpieczeństwo to nie tylko ochrona komputerów. To system naczyń połączonych – sieci, aplikacji, urządzeń, ludzi i procedur. Każdy element może stać się najsłabszym ogniwem. Niejednokrotnie przekonałem się, że to człowiek, nie technologia, stanowi główne wejście dla hakera.

Na czym polega ta dziedzina? Mówiąc najprościej, chodzi o zabezpieczanie systemów komputerowych, sieci i danych przed nieautoryzowanym dostępem, kradzieżą lub uszkodzeniem. Brzmi prosto, ale za tym kryje się cały wachlarz technik, narzędzi i metod. Od rozpoznania, przez testy penetracyjne, po monitorowanie i reagowanie na incydenty.

Wkraczając w ten świat, szybko zrozumiałem również, że istnieje podział ról. Możesz być pentesterem, czyli osobą symulującą ataki, by wykrywać słabości. Możesz dołączyć do zespołu Blue Team, który zajmuje się obroną i monitorowaniem systemów. Red Team to ci, którzy przeprowadzają realistyczne symulacje ataków, często nie informując Blue Teamu o swoich działaniach. Jest też Purple Team – most łączący czerwień i błękit, który analizuje wyniki obu stron, wyciąga wnioski i optymalizuje procesy.

Ja zaczynałem jako samouk, bawiąc się kodem i narzędziami, stopniowo poznając mechanizmy ataków i zabezpieczeń. Dziś wiem, że każdy, kto chce wkroczyć w tę branżę, powinien znać te podstawy:

1. Poufność – dane muszą być dostępne tylko dla uprawnionych osób.
2. Integralność – dane nie mogą być zmieniane bez autoryzacji.
3. Dostępność – systemy i usługi muszą być dostępne, gdy są potrzebne.

To tak zwana triada CIA (Confidentiality, Integrity, Availability), która jest kręgosłupem cyberbezpieczeństwa.

Zapamiętaj te zasady. To one będą Twoją tarczą, gdy wyruszysz w dalszą podróż. Ja też od nich zaczynałem. Gotowy, by wejść głębiej?