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?