Leszek Miś. Security Researcher oraz założyciel firmy Defensive-Security.com, specjalizującej się w dostarczaniu linuksowych usług, szkoleń i kursów z zakresu cyberbezpieczeństwa. Ma niemal 25-letnie praktyczne doświadczenie w działaniach ofensywnych i defensywnych z wykorzystaniem systemu Linux.

Główne obszary jego specjalizacji obejmują projektowanie wieloetapowych ścieżek ataku w ramach emulacji atakujących, inżynierię detekcji, ekstrakcję cech i artefaktów powłamaniowych, wyszukiwanie zagrożeń oraz walidację poprawności działania systemów EDR/Runtime/SIEM.

Entuzjasta rootkitów działających w przestrzeni użytkownika, jądra oraz eBPF, a także ciekawych implementacji C2. Na bieżąco skupia się na wyszukiwaniu nowych technik ofensywnych w systemach Linux oraz środowiskach Kubernetes, zawsze w ścisłym powiązaniu z metodami wykrywania, reagowania i ochrony.

WSTĘP

Na rynku istnieje wiele merytorycznych książek dotyczących szeroko pojętego bezpieczeństwa Linuksa. Do dyspozycji mamy zarówno pozycje mniej, jak i bardziej zaawansowane technicznie, takie, które są jedynie skromnym przewodnikiem, albo wyglądające jak Biblie: szczegółowe i mocno osadzone w kontekście.

Dla początkujących w tym temacie są wydania, które w metodyczny sposób omawiają podstawy oraz zaawansowane aspekty architektury systemu Linux i poszczególnych komponentów w warstwie jądra i przestrzeni użytkownika. Mamy do dyspozycji książki poświęcone utwardzaniu i bezpiecznej konfiguracji systemu oraz zabezpieczaniu elementarnych usług systemowo-sieciowych. Solidnych dzieł o atakowaniu i obronie, o podejściu *Active Defense*, analizie powłamaniowej czy ćwiczeniach typu *purple teaming* również powstało wiele. To tylko przykłady tej, dostępnej od ręki (jednego kliknięcia?), różnorodności.

Jeśli jednak jesteś ekspertem z niemal 25-letnim doświadczeniem, z pewnością masz ochotę „zejść jeszcze niżej" i poczytać książki traktujące o konkretnych zagadnieniach, np. o analizie formatu plików ELF czy postincydentalnej analizie pamięci RAM, metodach eksploitacji jądra, rozumieniu działania i sposobach omijania systemów EDR/Runtime Security. Możesz również chcieć zapoznać się z obszarem obsługi incydentów, z inżynierią detekcji, budową od podstaw logik detekcyjnych na bazie reguł Sigma, tworzeniem polityk SELinux, ich implementacją i utrzymaniem, często z uwzględnieniem ekosystemu SIEM. Tych pozycji także jest sporo.

Nie mogę też nie wspomnieć o książkach omawiających zakres implementacji i wykorzystania narzędzi *blue team* – warte wymienienia w tym miejscu są szczególnie te skupiające się na ujęciu obszaru walidacji poprawności działania i badaniu pokrycia detekcji w bezpośrednim ujęciu ofensywnym na podstawie MITRE ATT&CK® Framework, czego sam osobiście jestem wielkim fanem.

W żadnym wypadku nie można pominąć także istotności infrastruktury chmurowej, stanowiącej dodatkowy aspekt, z którym musimy być zaznajomieni, nie zapominajmy zatem zarówno o chmurach publicznych i prywatnych, jak i o poszczególnych usługach interchmurowych – często w ujęciu linuksowym – o tym także wydano już setki ciekawych pozycji.

Wobec takiej mnogości literatury na temat Linuksa można zatem zadać pytanie, po co powstała następna książka o jego bezpieczeństwie. Czy warto kolejny raz

poświęcić czas na czytanie materiału, który niejednokrotnie był już wcześniej opisywany w różnych ujęciach i indywidualnych stylach przez autorów/specjalistów na całym świecie? Książek uwzględniających wiele różnych podejść, poziomów zaawansowania i szczegółowości środowiska Linux?

Widzę dwie odpowiedzi na te pytania i spróbuję obiektywnie je tu uzasadnić.

Pierwsza z nich – uwielbiana szczególnie przez pentesterów i badaczy bezpieczeństwa – brzmi: „to zależy". W naszym środowisku, w tym konkretnym kontekście, wszystko zależy od tego, czego faktycznie poszukujesz, co interesuje Cię najbardziej, jakie są obecnie Twoje umiejętności i w którym kierunku potrzebujesz i chcesz się dalej rozwijać.

W tym miejscu, z dwóch różnych perspektyw odwołujących się do Twojego aktualnego doświadczenia, postaram się przedstawić korzyści, które może przynieść przeczytanie tej książki. Wezmę najpierw pod uwagę dwa poziomy wiedzy: Czytelnika początkującego, z rokiem–dwoma latami doświadczenia w środowisku Linux, oraz eksperta, tzw. wyjadacza, z ponad dekadą aktywnego „klikania".

Druga odpowiedź, znajdująca się nie bez powodu na końcu tego krótkiego *Wstępu*, będzie może w pierwszej chwili trochę zaskakująca, ale dla mnie jako Czytelnika tej książki jest niemniej istotna.

DLACZEGO Z LEKTURY TWIERDZY... SKORZYSTA POCZĄTKUJĄCY?

Osobiście czytałem o architekturze, uczyłem się podstawowych komend linuksowych oraz zasad działania technik ofensywnych „na sucho", zanim jeszcze w domu pojawił się mój pierwszy PC. Już wtedy wiedziałem, że z Linuksem chcę dosłownie „iść przez życie", jednak początki wcale nie były łatwe. Przytłaczająca wręcz ilość poleceń i konfiguracji często generowała coraz to nowe pytania, zgodnie z powiedzeniem: „Im więcej wiesz, tym bardziej zdajesz sobie sprawę, że nic nie wiesz".

W środowisku Linux (jak zresztą w całym IT) ta sentencja sprawdza się doskonale – i jest to pierwszy argument przemawiający za tym, dlaczego warto przeczytać tę książkę.

My wszyscy, linuksowcy z tzw. zajawką czy freakowym podejściem, cechujemy się ogromnym apetytem na ciągłą eksplorację i poszerzanie wiedzy. Chcemy wiedzieć, co działa, jak działa i dlaczego działa w taki, a nie inny sposób. Poszukujemy dróg, które mają spełniać założenia i prowadzić do obranych celów.

Twierdza... w tym obszarze pozwala zrozumieć cały ekosystem, często w ujęciu niezwykle szczegółowym lub punktowo, skupiając się na istotności danej zmiennej konfiguracyjnej w bardzo specyficznym kontekście. Wystarczy zerknąć do spisu treści, aby przekonać się, że pozycja, którą czytasz, omawia najistotniejsze obszary z perspektywy administratora/właściciela środowiska, systemu, aplikacji w XXI wieku, w którym system Linux – mimo iż często niewidoczny – występuje praktycznie w każdej infrastrukturze produkcyjnej.

Oczywiście, jak już wspominałem, dla każdego interesująca może okazać się zupełnie inna część tej książki. Wierzę jednak, że dla początkujących, „czytana od

deski do deski", może stać się swoistym drogowskazem na drodze do zrozumienia, z czego składa się Linux, ale również do zaznajomienia się z obszarami dotyczącymi ataku, detekcji, obrony i hardeningu.

Kontekstowe nawiązywanie do przykładowych sposobów wykorzystania błędów konfiguracyjnych czy podatności doskonale łączy się z podstawami obsługi incydentów, znaczenia analizy logów, wczesnego wykrywania intruzów czy też proaktywnego badania pokrycia detekcji.

Dlatego, jeśli pozwolisz, zarekomenduję Ci coś od siebie: jeśli jesteś na początku przygody z Linuksem, przeczytaj tę książkę nie raz i nie dwa. Przeczytaj ją wielokrotnie, wracając do rozdziałów, które interesują Cię najbardziej. Jestem przekonany, że rozległa wiedza Autora, ciekawe komentarze i historie z życia wzięte, częste skupianie uwagi na drobnych szczegółach sprawią, że zarazisz się tytułową dociekliwością. Bo generalnie o skupienie się na szczegółach tutaj chodzi.

Naturalnie od samego czytania nie staniesz się ekspertem, dlatego instaluj już teraz swoją pierwszą maszynę wirtualną z Linuksem i odkrywaj wraz z Autorem świat pełen ciekawostek, powiązań i zależności. Najprościej będzie, gdy spróbujesz wykonywać polecenia równolegle z lekturą danego rozdziału, obierając drogę praktyczną. Pamiętaj, że finalnie liczy się głównie praktyka i brak ograniczeń w uzyskiwaniu odpowiedzi na zadawane sobie pytania. Czytając *Twierdzę...*, poznasz świat Linuksa i cały ekosystem otwartego oprogramowania jako przestrzeń niezliczonych możliwości oraz swego rodzaju kompas pomagający namierzać zakres bezpiecznej konfiguracji i istniejących zagrożeń, wektorów ataków i kontekstowego, szerokiego wachlarza ofensywności.

Na koniec, pamiętaj, aby się nie zrażać, jeśli czasami będzie Ci trudno zrozumieć, co Autor miał na myśli. Czytaj, eksploruj, analizuj linki z przypisów (koniecznie sprawdź, przy drugim podejściu, dokąd Cię posyła tymi ścieżkami!), ćwicz praktycznie, zachowaj wytrwałość. To podróż składająca się z wielu przystanków i potrzeby obierania często nowych kierunków i świeżego spojrzenia. Linux jest tego świata podstawą i wierzę, że i Ty odnajdziesz tu swoją indywidualną drogę, a ta książka w znaczący sposób Ci w tym pomoże.

TWIERDZA... DLA EKSPERTA

Jak już wspominałem, sam mam prawie 25 lat doświadczenia w pracy z systemem Linux, głównie w zakresie cyberbezpieczeństwa. Zapytany o to, nazywam siebie badaczem bezpieczeństwa i architektem rozwiązań *open source*. Moje serwery oparte są naturalnie na Linuksie. To samo dotyczy wirtualnych maszyn, środowiska labowego, które również bazuje głównie na otwartym oprogramowaniu. Na desktopie, niezmiennie od kilkunastu lat, też mam zainstalowanego Linuksa. Moja Żona i Syn również korzystają z tego systemu. Komercyjnie dostarczam usługi z zakresu zaawansowanych ćwiczeń *red vs blue*, hardeningu środowisk oraz integracji i utrzymywania rozwiązań typu EDR/Runtime Security dla środowiska Linux. Szczególną uwagę poświęcam walidacji pokrycia detekcji tychże silników EDR/Runtime, zrozumienia, jak faktycznie się one zachowują oraz jak skorzystać z nich w ramach

realnej obsługi incydentów. Wszystko to sprowadza się do aktywnej i nieustannej analizy ekosystemu zagrożeń i praktycznego uruchamiania technik ofensywnych. W ramach treningów i szkoleń przeprowadzanych na żywo (dla klientów na całym świecie) uwielbiam schodzić do warstwy wywołań systemowych, analizować ciekawe i przede wszystkim aktualne techniki oraz trendy ofensywne wraz z korespondującym obszarem detekcyjno-śledczym. Droga, którą obrałem kilka lat temu – fachowo nazywana *purple teaming* – pozwala mi dzisiaj jednocześnie patrzeć na zachowanie danej instancji systemu operacyjnego Linux z dwóch powiązanych ze sobą perspektyw: ofensywnej i defensywnej.

Mam więc swoje doświadczenia i istotnie, dość spore wymagania merytoryczne od pozycji, którą zamierzam zakupić. I tu pojawia się kolejny argument, który przemawia za przeczytaniem tej książki także przez zaawansowanych i doświadczonych „graczy". *Twierdza…* w bardzo przystępny, a jednocześnie mocno merytoryczny sposób przedstawia aspekty bezpieczeństwa Linuksa. Czytając ją jako recenzent, z zarysowanym powyżej własnym linuksowym portfolio, nie zawiodłem się na Autorze, który napisał ją także dla mnie.

Ogromna liczba projektów i linków zewnętrznych, sporo świeżych wzmianek o nowych funkcjonalnościach w solidnych projektach, z których korzystamy od lat (takich jak np. `PerSourcePenalties` w OpenSSH 9.8), solidne spojrzenie na proces uruchamiania systemu czy architektury LUKS „rozwala mózg". Nawiązywanie do rootkitów różnych warstw czy C2, ukierunkowanie na zapoznanie się z technologią eBPF – zarówno pod kątem defensywnym, jak i ofensywnym – to wisienki na torcie. Są one „rozsypane" na kartkach tej książki, więc doświadczony znawca Linuksa ciągle czuje się jak… ich odkrywca.

Świetnie przedstawione zarządzanie usługami, omówione LSM-y, wzmianki o rozwiązaniach do monitorowania bezpieczeństwa środowiska Kubernetes, ogromna liczba różnego rodzaju poleceń z niekoniecznie oczywistymi parametrami. Całość w konwencji – trudno tu znaleźć jedno właściwe słowo – „adminowo-bezpiecznikowej", z bagażem doświadczeń ze sporego kawałka życia Autora (o czym jeszcze napiszę poniżej). Do tego kontekstowe nawiązywanie do popełnionych kiedyś przez niego błędów stanowi dodatkową wartość samą w sobie. Mówiono nam: „ucz się na błędach", a zawartość *Twierdzy…* jest tego zalecenia najlepszą, wciągającą formą. Jestem przekonany, że każdy znajdzie w tej książce coś ciekawego i nowego.

Jak już wspomniałem, wszyscy stale chcemy, ale też i musimy uczyć się nowych rzeczy, a ta publikacja zdecydowanie zachęca do zgłębiania i dalszej eksploracji. Sam też już nie mogę się doczekać, gdy zainspirowany tą lekturą zanurzę się w budowanie kolejnej ścieżki ataku linuksowego, uwzględniającej np. zdalną eksploitację podatności w Redis (CVE-2025-49844), *filelessowe* uruchamianie implantu frp[1] dostarczającego funkcjonalność SOCKS Proxy i nawiązującego połączenie na bazie nieoczywistego KCP/UDP, zainstalowanie persystencji wykorzystującej `udev`, dostarczenie tzw. funkcjonalności *magic-packet* z wykorzystaniem ofensywnego eBPF czy ukrycie wszelkich powiązanych procesów/artefaktów za pomocą *hookowania syscalli* z wykorzystaniem tym razem rootkita warstwy LKM o nazwie Singularity[2], ładowanego także bez dotykania dysku. A całość, w ramach ćwiczenia *red vs*

blue, wykrywana będzie z uwzględnieniem stosu technologicznego zawierającego komponenty takie jak: Falco[3], Kunai[4], OSquery Defense Kit[5], Velociraptor[6], Elastic[7], UAC[8], bpftool[9], ghostscan[10], Volatility3 Framework[11], Zeek[12] i Suricata[13] oraz oczywiście kawałka spoiwa w postaci „magii" konsolowej w ujęciu analizy `/proc` i `/sys`.

Brzmi jak zajawka? Czytaj *Twierdzę…* i zaraź się! Dla mnie, po jej lekturze, to jedna z wielu zawodowych inspiracji płynących z doświadczenia jej Autora.

NIE MA NA TYM ŚWIECIE CZŁOWIEKA, KTÓRY O LINUKSIE WIE WSZYSTKO

Powracając do podstawowego pytania, czy warto przeczytać tę książkę, druga nasuwająca mi się na myśl odpowiedź wiąże się z refleksją, że to także opis „wyjątkowej Karola podróży przez życie" z bezpieczeństwem Linuksa, którą możesz poczuć na własnej skórze, właśnie czytając *Twierdzę…* Jako pasjonat z wieloletnim doświadczeniem przy konsolach linuksowych najróżniejszych dystrybucji dokładnie w ten sposób odebrałem książkę, którą trzymasz w rękach. I stanowi to, oprócz wartości *stricte* merytorycznej, istotnie łakomy kąsek z perspektywy czysto życiowej, a w pewnym sensie również psychologicznej, co jest ogromną zaletą tej pozycji.

W tym miejscu przypomniała mi się sytuacja jeszcze z czasów technikum elektronicznego, którego byłem uczniem. Podczas lekcji języka polskiego, prawdopodobnie w III lub IV klasie, mieliśmy za zadanie opisać wizję swojej zawodowej przyszłości. Pamiętam, że w mojej pracy napisałem już wtedy: „chciałbym zostać ekspertem ds. bezpieczeństwa systemu Linux i wiedzieć na jego temat wszystko i znać każdy jego szczegół". To, co zapamiętałem z tej lekcji, to świadomy komentarz nauczycielki, brzmiący mniej więcej w ten sposób: „Leszku, pamiętaj, że nie ma na tym świecie człowieka, który o Linuksie wie wszystko". Te słowa są ze mną do dziś, a ja nadal się uczę. W ostatnim rozdziale, a konkretnie w części *Bądź dla siebie człowiekiem*, znajduje się zbiór niezwykle cennych, życiowych wskazówek, które osobiście bardzo sobie cenię. Przyznam tutaj, że sam przeżyłem niejedną burzę, sztorm czy nawet życiowy huragan piątej kategorii, może nawet podobnie jak Ty. W moim przypadku „zajawka" linuksowa sama w sobie nie była ich bezpośrednim powodem, ale z wiekiem faktycznie nauczyłem się, że metoda małych kroczków, sport, zdrowa dieta i odpowiednia dawka snu to podstawa, aby pozostać w tej cudownej, linuksowej podróży.

Zatem, wytrwale, małymi kroczkami – pamiętaj! – to jest ważne przesłanie tej książki, bo nie uda się jej przeczytać na jednym oddechu. Trzeba będzie wracać, żeby pogłębiać zdobywaną wiedzę.

Polecam ją więc w tym miejscu bardzo świadomie.

Chciałbym też na jej kartach otwarcie pogratulować Karolowi, że ją napisał, i jednocześnie podziękować za możliwość wczesnego recenzowania, jak i dodania kilku słów od siebie w ramach tego *Wstępu*.

Wykonałeś kawał dobrej roboty! To bardzo osobista książka na bardzo techniczny temat. Bądź z siebie dumny i podążaj dalej w zdrowiu, z frajdą i zamiłowaniem, jakie jest zdecydowanie wyczuwalne w każdej linijce Twojego tekstu. Niech moc będzie z Tobą! Niech pakiety i *syscalle* pozostaną pod Twoją kontrolą!

PRZYPISY

twierdza.sekurak.pl/r0

1 fatedier, *frp*, GitHub, https://github.com/fatedier/frp
2 MatheuzSecurity, *Singularity – Stealthy Linux Kernel Rootkit*, GitHub, https://github.com/MatheuZSecurity/Singularity
3 falcosecurity, *Falco*, GitHub, https://github.com/falcosecurity/falco
4 Kunai Project, *Kunai*, GitHub, https://github.com/kunai-project/kunai
5 Chainguard, *osquery-defense-kit*, GitHub, https://github.com/chainguard-dev/osquery-defense-kit
6 Velocidex, *Velociraptor – Endpoint visibility and collection tool*, GitHub, https://github.com/Velocidex/velociraptor
7 *Elastic*, https://www.elastic.co/security
8 Lahr T.C. (tclahr), *UAC*, GitHub, https://github.com/tclahr/uac
9 libbpf, *bpftool*, GitHub, https://github.com/libbpf/bpftool
10 h2337, *ghostscan*, GitHub, https://github.com/h2337/ghostscan
11 Volatility Foundation, *Volatility 3: The volatile memory extraction framework*, GitHub, https://github.com/volatilityfoundation/volatility3
12 Zeek Network Monitoring Project, *Zeek*, GitHub, https://github.com/zeek/zeek
13 Open Information Security Foundation (OISF), *Suricata*, GitHub, https://github.com/OISF/suricata