ADAM ZIAJA

PRAKTYCZNA ANALIZA POWŁAMANIOWA

APLIKACJA WEBOWA W ŚRODOWISKU LINUX

PWN

ADAM ZIAJA

PRAKTYCZNA ANALIZA POWŁAMANIOWA

APLIKACJA WEBOWA W ŚRODOWISKU LINUX

PWN

Projekt okładki i stron tytułowych **Hubert Zacharski**

Projekt okładki i stron tytułowych **Shutterstock/ Sky Designs, Shutterstock/ Alexey Godzenko**

Wydawca **Łukasz Łopuszański**

Redaktor prowadzący **Adam Kowalski**

Redaktor **Irena Puchalska**

Koordynator produkcji **Anna Bączkowska**

Recenzent **Dr hab. inż. Jerzy Kosiński**

Skład wersji elektronicznej na zlecenie Wydawnictwa Naukowego PWN **Marcin Kapusta / konwersja.virtualo.pl**

eBook został przygotowany na podstawie wydania papierowego z 2017 r., (wyd. I)
Warszawa 2017

ISBN 978-83-01-19605-9

Wydawnictwo Naukowe PWN SA
tel. 22 69 54 321, faks 22 69 54 288
infolinia 801 33 33 88
e-mail: pwn@pwn.com.pl; reklama@pwn.pl
www.pwn.pl

Spis treści

1.
Wstęp

Informacje zawarte w tej książce pokazują podejście autora do analizy powłamaniowej w odniesieniu do przypadku nieautoryzowanego dostępu i naruszenia integralności strony internetowej oraz tematów pokrewnych z tego wynikających. Podejście to jest oparte na praktycznym doświadczeniu oraz powszechnie wykorzystywanych standardach. Atakujący kierują się własnym podejściem oraz często wykorzystują zaawansowane i kreatywne sposoby działania, zarówno samego ataku, jak i zacierania śladów. Nie istnieją uniwersalne sposoby analizy powłamaniowej gwarantujące uzyskanie oczekiwanych rezultatów. Z oczywistych więc względów w książce nie opisano wszystkich możliwości analizy powłamaniowej, tak samo jak w książkach o programowaniu nie da się opisać sposobu kodowania każdego rodzaju programu. Nie powinno się ślepo wierzyć w znalezione informacje, lecz starać się je weryfikować w innych miejscach, jeśli są istotne dla analizy. Wszystkie czasy MAC[1] w systemie plików mogą być sfałszowane, a pliki podmienione, mimo braku zmiany numerów inode[2] – to tylko jedne z wielu trików wykorzystywanych przez atakujących. Dlatego ufaj, ale weryfikuj. Jeśli uda nam się szybko znaleźć tylną furtkę w systemie, nie oznacza to, że atakujący nie był na tyle sprytny, by celowo ją zostawić. Mógł to zrobić po to, by nie doszło do dalszej wnikliwej analizy, a w efekcie wykrycia pozostawionego przez niego rootkita. Analiza powłamaniowa to sztuka szukania potknięć atakującego.

Jedynym bezpiecznym rozwiązaniem po ujawnieniu włamania jest w rzeczywistości pełna reinstalacja systemu[3] oraz niewykorzystywanie zasobów, takich jak na przykład skompilowane na skompromitowanym systemie programy, czy też innego rodzaju dane z niego pochodzące, o ile nie zostały należycie zweryfikowane. Jednak celem informatyki śledczej

jest analiza danych stanowiących potencjalny dowód nadużyć. Pozwala z założenia odpowiedzieć na pytania, co się właściwie stało, jak doszło do włamania i kto jest za nie odpowiedzialny. Treść niniejszej książki jest związana z pojęciem DFIR (*Digital Forensics and Incident Response*) – częściowo zajmuje się informatyką śledczą, a częściowo tematem reagowania na incydenty.

Tematyka DFIR jest bardzo rozległa i zazwyczaj rozpatrywana w odniesieniu do systemu Windows. Brakuje opracowań związanych z systemem Linux, szczególnie pod kątem analizy powłamaniowej, i dlatego, bazując na doświadczeniu zawodowym, powziąłem zamiar stworzenia takiej książki. Wbrew pozorom, wszystkie zawody informatyczne są ze sobą mocno powiązane i zróżnicowana wiedza pozwala wyciągać bardziej trafne wnioski przy wykonywaniu prac związanych z bezpieczeństwem IT. Szczególnie w przypadku aspektów bezpieczeństwa nie są to zupełnie odrębne dziedziny, o czym należy pamiętać – na przykład nie da się w pełni rozumieć pracy na stanowisku pentestera (testera penetracyjnego), nie mając chociaż podstawowej wiedzy związanej z systemami, sieciami oraz programowaniem. Nie da się przeprowadzić rzeczowej analizy powłamaniowej bez mocnych podstaw z dziedziny testów penetracyjnych i wiedzy o analizowanym systemie operacyjnym. Wynika to z faktu, że analizując, można trafić na ślady włamania i nawet nie zdawać sobie z tego sprawy, co wbrew pozorom jest dość częstym problemem. Informatyka śledcza nabiera coraz większego znaczenia, do naszego życia wkraczają bowiem kolejne zinformatyzowane systemy, a wraz z rozwojem technologicznym liczba ataków będzie coraz większa. Należy pamiętać, że w Internecie każdy otrzymał darmowy test penetracyjny, tylko nie każdy dostał z niego raport[4]…
Dla kogo więc tak naprawdę jest ta książka? Praktycznie dla wszystkich zainteresowanych bezpieczeństwem IT. Informatycy śledczy i biegli sądowi skorzystają z informacji w niej zawartych pod kątem możliwości analizy śladów oraz wyciągania kolejnych istotnych informacji. Specjaliści bezpieczeństwa pracujący w zespołach typu SOC czy CERT (CSIRT) z kolei uzupełnią swoją wiedzę związaną z reagowaniem na incydenty, w tym zapoznają się z możliwościami live forensics oraz technikami zabezpieczania nośników cyfrowych, aby stanowiły wartość dowodową. Z

kolei osoby zajmujące się autoryzowanymi atakami dowiedzą się, jakie informacje można ustalić oraz co robić, aby nie zostawiać śladów. Takie wiadomości niewątpliwie przydadzą się w rozwijającej się w ostatnim czasie dziedzinie, jaką jest red teaming[5].

Pomysł na stworzenie tej książki zrodził się w chwili, kiedy zostałem poproszony o napisanie w punktach, jak będzie wyglądała moja analiza włamania na serwer przez aplikację webową. W pierwszej chwili wydawało mi się to oczywiste. Po głębszym jednak zastanowieniu doszedłem do wniosku, że to pytanie rodzaju: jakie znasz kolory, a nam co chwilę przypominają się następne. Innymi słowy, nie wiadomo od czego zacząć, ponieważ w przypadku analizy powłamaniowej nie istnieją żadne konkretne i techniczne szeroko uznane metodyki jak to ma miejsce na przykład w przypadku testów bezpieczeństwa aplikacji webowych i metodyki OWASP (*Open Web Application Security Project*). W Internecie co prawda można znaleźć wiele poradników o tym, co robić po incydencie, pod kątem analizy powłamaniowej, ale zwykle proponują one niestety błędne podejście.

Pisząc tę książkę, starałem się, aby była jak najbardziej techniczna oraz aby czytając ją, nie trzeba było korzystać z mazaka do zakreślania istotnych fragmentów. Dlatego znalazło się w niej niewiele obszernych opisów i całość została napisana w stylu techbloga – ma charakter technicznego artykułu z branżowego internetowego serwisu. Nie rozwijałem również zbytnio tematów, które były już wielokrotnie omawiane i kolejny opis nic nowego by nie wniósł. Dlatego też na próżno szukać tutaj omówień systemów plików, historii informatyki śledczej czy instrukcji instalacji systemu Linux. Innymi słowy, czytelnik znajdzie w niej przede wszystkim esencję istotnych informacji.

Strona internetowa, błędy oraz errata

Bardzo bym chciał, aby ta książka była wolna od błędów, ale zakładam, że – jak to bywa z technicznymi książkami – czytelnicy prawdopodobnie je znajdą. Dlatego proszę o zgłaszanie wszelkiego rodzaju błędów, a

szczególnie merytorycznych. Errata oraz podziękowania za zgłoszenia będą opublikowane pod adresem:

http://adamziaja.com/book/

Pod tym adresem znajdą się również wszelkie informacje związane z książką, jak na przykład repozytorium kodu.

W treści książki znajdują się odnośniki do tej strony kończące się „losowymi” znakami, przekierowujące do właściwej treści. Z jednej strony pełni to funkcję skracacza adresów (wystarczy przepisać kilka znaków na koniec stałego adresu), a z drugiej, co bardziej istotne, pozwoli mi zareagować, gdy adres przestanie działać. Będę mógł wtedy przekierować na nowy adres lub zarchiwizowaną treść albo też na zupełnie inną stronę zawierającą zbliżoną zawartość do pierwotnego przekierowania.

O autorze

Adam Ziaja jest związany z bezpieczeństwem IT od kilkunastu lat, swoją karierę zawodową zaczynał od administracji systemami Linux w największym polskim portalu internetowym. Następnie pracował jako informatyk śledczy, tworząc ekspertyzy dla organów ścigania oraz wymiaru sprawiedliwości. Zajmował się przy tym głównie cyberprzestępczością i brał udział w zabezpieczaniu sprzętu komputerowego na miejscu przestępstw. Kolejnym krokiem w karierze była praca w zespole CSIRT (*Computer Security Incident Response Team*), gdzie zajmował się reagowaniem na incydenty naruszenia bezpieczeństwa oraz CTI (*Cyber Threat Intelligence*). Był członkiem zwycięskiej drużyny w największych europejskich cywilnych ćwiczeniach z zakresu ochrony cyberprzestrzeni Cyber Europe 2014. Jest współautorem materiałów dydaktycznych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) dla zespołów CERT poświęconych m.in. informatyce śledczej oraz wykrywaniu i zwalczaniu cyberprzestępczości. Regularnie, od paru lat jest prelegentem na międzynarodowej konferencji naukowej Techniczne Aspekty Przestępczości Teleinformatycznej (TAPT) organizowanej przez Wyższą Szkołę Policji w Szczytnie. Od kilku lat zajmuje się przede wszystkim ofensywnym bezpieczeństwem teleinformatycznym, przeprowadzając legalne, autoryzowane ataki w postaci testów penetracyjnych oraz red teamingu głównie dla podmiotów wchodzących w skład infrastruktury krytycznej. Prywatnie zajmuje się bug huntingiem, za co otrzymał dziesiątki podziękowań od instytucji z całego świata, m.in. Adobe, Apple, BlackBerry, Deutsche Telekom, eBay, Harvard University, Nokia, VMware, Yahoo, Yandex, jak również polskich, takich jak Onet, Interia, Wirtualna Polska oraz Empik. Jest członkiem grupy non profit MalwareMustDie zrzeszającej osoby aktywnie zwalczające internetowe zagrożenia. Ma status biegłego sądowego z listy Sądu Okręgowego w Warszawie z zakresu informatyki, a szczególnie informatyki śledczej,

analizy powłamaniowej w systemach Linux, hackingu i cyberprzestępczości. Posiada certyfikaty z zakresu praktycznych sieciowych ataków, m.in. *Offensive Security Certified Professional* (OSCP), *Offensive Security Wireless Professional* (OSWP) oraz *eLearnSecurity Web application Penetration Tester* (eWPT).

Strona internetowa – http://adamziaja.com
E-mail – adam@adamziaja.com

Podziękowania

Chciałbym serdecznie podziękować osobom, które przyczyniły się do recenzji merytorycznej oraz poprawy niedociągnięć, a byli nimi szczególnie: Dawid Skomski, Artur Byszko, Jerzy Kosiński, Paweł Wyleciał, Dawid Osojca, Kacper Szurek, Mateusz Krzywicki, Dorota Kulas, Błażej Kantak, Krystian Mączka, Daniel Suchocki, Gynvael Coldwind oraz Adam Zabrocki.

Podziękowania należą się również Wydawnictwu Naukowemu PWN, a w szczególności wydawcy Łukaszowi Łopuszańskiemu i redaktorowi prowadzącemu Adamowi Kowalskiemu.

2.
Zabezpieczanie danych

Zabezpieczanie danych ma różny przebieg, zależnie od podejścia. Zgodnie z terminem DFIR są dwa podstawowe: jedno tradycyjne – od strony informatyki śledczej, a drugie – od strony reagowania na incydenty.

Jeśli podchodzimy do sprawy zgodnie z dobrymi praktykami, w myśl zasad informatyki śledczej, to powinna zostać wykonana kopia binarna (1:1) wraz z wygenerowaniem sumy kontrolnej, a wszelkie przyszłe prace powinny być wykonywane na kopii. Najlepiej posiadać dwie kopie: główną oraz tę, na której będą prowadzone badania. Podejście to jest związane z realnym ryzykiem, że podczas analizy – ze względu na duże obciążenie w postaci ciągłego odczytu – dysk może ulec fizycznemu uszkodzeniu. W trakcie wykonywania kopii binarnej dysk dowodowy powinien być podłączony do komputera – na którym jest wykonywana kopia – za pośrednictwem urządzenia blokującego zapis, tzw. bloker[6]. Jest to dedykowane urządzenie analizujące komendy ATA/SATA przesyłane do kontrolera dysku i blokujące wszelkie próby dokonania przez system zapisu na dowodowym nośniku. Gwarantuje to nam integralność i unikamy ryzyka przypadkowej zmiany danych na dysku dowodowym. Możliwe jest oczywiście uruchomienie i analiza dysku dowodowego, na przykład z systemu Live-CD, gdzie dysk dowodowy zamontowany będzie z opcją „tylko do odczytu”, jednak przy takim scenariuszu pracy może dojść do nieumyślnego uruchomienia systemu z dysku dowodowego zamiast z nośnika Live-CD. Przykładową konsekwencją takiej sytuacji jest modyfikacja czasów MAC lub też wykonanie różnego rodzaju skryptów startowych, czego efektem może być nadpisanie na dysku istotnych danych. Stosując bloker, nie martwimy się, że do takich incydentów dojdzie. Minusem wykonywania zabezpieczenia w sposób tradycyjny jest z

pewnością czas, który musimy na to poświęcić. Samo wykonywanie obrazu dysku może trwać wiele godzin, a dochodzi jeszcze indeksowanie jego zawartości, szukanie słów kluczowych itd. Ostatecznie, wszystkie czynności trwają zwykle kilka dni, zależnie od pojemności dysków i od tego, czego szukamy. Plusem z kolei jest dokładność analizy oraz integralność danych, dlatego ten rodzaj podejścia nie zostanie w pełni zastąpiony.

Z kolei podejście od strony reagowania na incydenty jest nastawione szczególnie na tzw. live forensics, czy też live response. W jego przypadku operujemy przede wszystkim na działającym komputerze. Metoda ta polega na wykonywaniu operacji bezpośrednio na analizowanym systemie: sprawdzaniu plików, połączeń sieciowych, kont użytkowników itd. Możemy też wykonać kopię dysku bez wyłączania komputera. Często w przypadku takiej analizy zabezpiecza się również zrzut pamięci RAM, ponieważ przechowywane są tam ulotne informacje pozwalające na odtworzenie stanu, w jakim komputer był w chwili wykonywania zrzutu. Jeśli zrobimy obraz dysku, a pominiemy zrzut pamięci, to utracimy informacje o portach otwartych w systemie czy działających procesach. Oczywiście takie informacje też można, przynajmniej częściowo odtworzyć z danych zapisanych na dysku, jednak jest to niewspółmiernie bardziej problematyczne niż badanie pamięci. Ten sposób ma swoje zalety w przypadku szyfrowanych dysków, ponieważ możemy uzyskać dostęp po pierwsze do odszyfrowanych danych i wykonać obraz aktualnego stanu nośnika, a po drugie istnieje możliwość odczytania kluczy szyfrujących z pamięci[7]. Live forensics ma niestety sporo minusów i wykonując jakiekolwiek operacje na dysku, jednocześnie ryzykujemy bezpowrotnym nadpisaniem istotnych informacji. Wykorzystując w trakcie analizy informacje z potencjalnie skompromitowanego systemu, narażamy się na możliwość, iż dane te mogą być sfałszowane na poziomie jądra systemu przez rootkita. Główną zaletą takiego podejścia w przypadku istotnych systemów, których niedostępność musi być minimalizowana, jest przede wszystkim brak konieczności wyłączania badanego komputera, jak również sam czas reakcji na incydent. Analizę przeprowadzamy w czasie rzeczywistym, a nie czekamy wiele godzin na kopię dysku i następnie jego indeksowanie, żeby w ogóle móc odpowiedzieć na podstawowe pytania

odnośnie do incydentu. W typowym reagowaniu na incydenty reakcja na zagrożenie powinna być natychmiastowa, szczególnie że zazwyczaj nie posiadamy zbyt wielu informacji na jego temat.

Pamiętajmy, że informatyka śledcza i reagowanie na incydenty to pojęcia, które ostatnimi czasy powoli się zacierają, stąd też jedno wspólne określenie DFIR. Zawsze szukamy podobnych artefaktów (śladów) w systemie, a ostatecznym celem jest analiza danych i odpowiedzi na pytania, z powodu których analiza była w ogóle wykonywana. Nic nie stoi zatem na przeszkodzie, aby łączyć te oba podejścia i często bywa, że informatyk śledczy wykonuje zrzut pamięci, a następnie robi kopię binarną. Minusem jest fakt działania na materiale dowodowym i jednoczesna ingerencja w niego. Biegły sądowy w uzasadnionych przypadkach może wykonać zrzut pamięci, co wiąże się bezpośrednio z naruszeniem integralności analizowanego systemu. W takiej sytuacji biegły wykonuje protokół z realizacji tych czynności, w którym znajdą się m.in. szczegółowe informacje o wykonanych operacjach oraz dokładne sygnatury czasowe. Jednak procedury pracy biegłych sądowych, a szczególnie procedury zabezpieczania materiału dowodowego na wniosek organów uprawnionych wykraczają poza tematykę tej książki.

Warto zwrócić uwagę, że nie istnieje złoty sposób zabezpieczenia komputera – szczególnie dotyczy to analizy powłamaniowej. W tym przypadku do procesu trzeba podejść indywidualnie i często liczyć na łut szczęścia, ponieważ każde działanie w trakcie zabezpieczania może wywołać niechciane konsekwencje. Generalną zasadą jest rozpoczynanie zabezpieczenia od danych najbardziej ulotnych. Jeśli zabezpieczamy komputer, na który się włamano, istnieje wiele potencjalnych problemów. Na początek możemy odłączyć kabel sieciowy, aby atakujący nie miał dostępu do komputera. Pojawi się jednak problem, że zainstalowane przez atakującego oprogramowanie może w odpowiedzi na to wykonać jakąś operację, na przykład zamknąć komputer przy zaszyfrowanych dyskach w celu wyłudzenia okupu. Wykonanie zrzutu pamięci mogłoby w takim przypadku ewentualnie pomóc uzyskać klucz szyfrujący. Nie wiemy jednak, czy próba wykonania zrzutu pamięci lub obrazu dysku, czy też odłączenie lub podłączenie czegokolwiek pod USB[8] nie spowoduje

jakiejś reakcji systemu. Sposobem może być odłączenie zasilania przez wyciągnięcie wtyczki z gniazdka, ponieważ oprogramowanie może też reagować na sygnał zamykania komputera. Taki sposób pozwala uniknąć reakcji logicznej oprogramowania, ale wraca problem potencjalnego szyfrowania dysku jak również utraty ulotnych informacji z pamięci RAM. W takim przypadku chociaż częściowo może nam pomóc analiza ruchu sieciowego. Jednak z uwagi, że zalogowanie się do systemu może pociągnąć za sobą jakąś reakcję, to operacja ta powinna być wykonana spoza analizowanego komputera. Możemy więc na przykład wykorzystać koncentrator (ang. *hub*) lub przeanalizować ruch sieciowy z poziomu rutera (trasownika, ang. *router*).

Dlatego każde zabezpieczanie komputera musi być rozpatrywane indywidualnie, szczególnie, jeśli istnieje uzasadnione ryzyko, że komputer został skompromitowany. W przypadku wirtualnych systemów największą zaletą jest możliwość wykonania migawki (ang. *snapshot*), czyli zapisania aktualnego stanu systemu – to zawsze będzie najlepsze, co możemy zrobić na początek.