Bezpieczeństwo systemów operacyjnych

Rejestrowanie zdarzeń

Arkadiusz Chrobot

Katedra Systemów Informatycznych

23 października 2026

Plan

1. Wstęp
2. Logi Windows
3. Logi Linuksa
4. Literatura

Wstęp

Rejestracja zdarzeń (ang. *even logging*) jest niezbędna nie tylko do ustalenia przyczyn awarii oprogramowania, ale także do wykrycia naruszeń bezpieczeństwa. W tym ostatnim aspekcie pomaga ona nie tylko odtworzyć działania adwersarza, ale także wykryć je w czasie rzeczywistym. Dlatego istotnym zagadnieniem jest nie tylko analiza dzienników zdarzeń (ang. *logs*), nazywanych żargonowo „logami", ale także zapewnienie ich integralności. Badanie logów może być dokonywane manualnie, z użyciem odpowiednich narzędzi, jak i całkowicie automatycznie, przez oprogramowanie typu SIEM (ang. *Security Information and Even Management*) lub EDR (ang. *Endpoint Detection and Response*). Informacje o zdarzeniach mogą być generowane zarówno przez oprogramowanie użytkowe, jak i przez system operacyjny, ale ze względu na rolę w systemie komputerowym to ten ostatni jest w dużej mierze odpowiedzialny za ich rejestrację oraz utrzymywanie i zarządzenie logami.

Logi Windows

Zdecydowana większość ▸ logów w systemie Windows jest zapisywana w plikach o formacie binarnym EVTX, choć bazującym jednocześnie na XML. Domyślnie są one zapisywane w katalogu o ścieżce `%SystemRoot%\System32\winevt\Logs\`. Trzy podstawowe z nich to:

Application Log zawiera informacje o zdarzeniach generowanych przez aplikacje,

System Log gromadzi informacje o zdarzeniach generowanych przez system Windows oraz jego usługi,

Security Log rejestruje informacje o operacjach związanych z bezpieczeństwem (uwierzytelnianie użytkowników, tworzenie kont, itd.)

Z punktu widzenia cyberbezpieczeństwa ostatni dziennik jest najbardziej pomocny, choć analiza incydentów powinna obejmować zawartość wszystkich.

Logi Windows

Zawartość dzienników w formacie EVTX można badać używając wyposażonego w GUI programu *Event Viewer* lub narzędzi korzystających z wiersza poleceń, takich jak `wevtutil` (CMD) lub `Get-EventLog` (PowerShell). Format wpisu do logu może być różny, w zależności od jego źródła i treści, ale zawsze występuje w nich identyfikator *Event ID*. O tym, które zdarzenia są rejestrowane stanowią ustawienia polityki GPO *Group Policy Object*, która może być określana globalnie, jeśli komputer pracuje w domenie, lub lokalnie. Warto przy okazji zaznaczyć, że jeśli maszyna z Windows jest pod kontrolą Active Directory, to część informacji o zdarzeniach może być odkładana w kontrolerze domeny. Domyślne ustawienia polityki gwarantują, że większość interesujących zdarzeń jest rejestrowana.

Logi Windows

Zarządzenie kontami

Zdarzenia dotyczące kont użytkowników i grup (dodanie, blokowanie, usunięcie, itp.) są domyślnie rejestrowane. Należy jednak zwrócić uwagę na rodzaj konta, np. informacje o utworzeniu konta domenowego zostaną zarejestrowane przez kontroler domeny, a nie lokalnie. Identyfikator zdarzenia w przypadku tych informacji jest czterocyfrowy i ma postać 47*xx*, przy czym identyfikatory części zdarzeń nie związanych z zarządzaniem kont też podlegają temu schematowi. Szczegółowość danych jest dosyć duża i obejmuje takie zdarzenia, jak dodanie użytkownika do lokalnej lub globalnej grupy zabezpieczeń, próba resetowania hasła, zablokowanie konta, itd.

Logi Windows

Logowanie

Dzienniki Windows rejestrują dwa typu zdarzeń związane z logowaniem: *logowanie do systemu*, czyli rozpoczęcie sesji na konkretnym komputerze i (jeśli komputer pracuje w domenie) *uwierzytelnienie konta*, czyli wydanie poświadczenia przez kontroler domeny w postaci biletu TGT (jeśli kontroler używa protokołu Kerberos). Oba wpisy są dodawane do dziennika bezpieczeństwa (Security Log).
Identyfikatory zdarzeń dla kont domenowych, podobnie jak dla zdarzeń związanych z zarządzaniem kont, podlegają wzorcowi 47*xx*. Dodatkowo, wśród danych rejestrowane są specyficzne dla protokołu Kerberos lub NTLM, jeśli zdarzenie tego wymaga.
Z kolei identyfikatory zdarzeń logowania interaktywnego, poza dwoma dotyczącymi RDP, podlegają schematowi 46*xx*. Tutaj również zbierane są dodatkowe informacje, np. typ udanego logowania (interaktywne, sieciowe, logowanie usługi, itd.).

Logi Windows

Dostęp do udziałów sieciowych

Domyślnie Windows rejestruje jedynie fakt logowania do udziałów. Można jednak rozszerzyć zakres odnotowywanych danych zmieniając ustawienia GPO (*Advanced Audit Policy→Object Access→Audit File Share*). Po tej zmianie będą również odkładane w Security Log informacje o uzyskaniu dostępu do udziału, utworzeniu nowego, zmianie uprawnień oraz usunięciu udziału. Zarejestrowanie informacji o tym, które konkretnie pliki są/były otwierane wymaga skorzystania z danych audytowych dla systemu plików NTFS.

Logi Windows

Zadania harmonogramu

Dla zadań wykonywanych według harmonogramu system Windows prowadzi osobny dziennik, który jest plikiem o nazwie `%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx`. Z poziomu programu *Even Viewer* jest on dostępny w *Application and Services Logs*→*Microsoft*→*Windows*→*TaskScheduler*→*Operational*. Podobnie jak w przypadku dostępu do udziałów sieciowych, rejestry te nie są zbyt szczegółowe, ale można to zmienić opcją *Enable All Tasks History* lub posługując się poleceniem `wevtutil`. Warto skorzystać z tej możliwości, bo harmonogram zadań jest często wykorzystywany przez adwersarzy do utrzymania dostępu do systemu z użyciem techniki *Living off the Land (LOTL)*, czyli przy wykorzystaniu dostępnych, zainstalowanych i niewzbudzających podejrzeń narzędzi, zamiast specjalizowanych programów do włamań.

Logi Windows

Zadania harmonogramu

Identyfikatory dla zdarzeń dotyczących zadań harmonogramu są trzycyfrowe i dotyczą takich operacji jak utworzenie nowego zadania, zmiana (aktualizacja) zdania, usunięcie zadania, wykonanie i zakończenie zadania. Warto zauważyć, że dane zdarzenia wykonania zadania (kod 200) obejmują także pełną ścieżkę dostępu do programu, który został wykonany w ramach zdania. Pozwala to wykryć np. próbę uruchomienia fałszywej usługi, której nazwa pliku wykonywalnego jest taka sama jak w przypadku legalnej, ale jest on umiejscowiony w nietypowym katalogu.

Logi Windows

Dostęp do obiektów

Domyślnie zdarzenia dostępu do obiektów, takich jak pliki i katalogi nie jest rejestrowany, z powodu dużej ilości danych, które należy zarejestrować. Warto jednak rozważyć włączenie mechanizmu za to odpowiedzialnego, czyli *Audytu dostępu do obiektów* (ang. *Object Access Audit*), jeśli w komputerze znajdują się cenne dane w takich strukturach. Wymaga to dwóch kroków. Najpierw trzeba zmienić ustawienia polityki GPO: *Security Settings*→*Local Policies*→*Audit Policy*→*Audit Object Access*. Następnie trzeba wskazać, które obiekty powinny być monitorowane, aby informacje o zdarzeniach ich dotyczących trafiały do dziennika bezpieczeństwa. Tę operację można wykonać włączając odpowiednią opcję w właściwościach pliku lub katalogu (*Zabezpieczenia*→*Zaawansowane*→*Audyt*).

Logi Windows

Dostęp do obiektów

Po wykonaniu kroków z poprzedniego slajdu w Security Log odnotowywane są dodatkowe dane dotyczące zadań harmonogramu oraz zdarzenia dotyczące *uchwytów* do obiektów, takich jak pliki, katalogi i klucze rejestru. Identyfikatory tych zdarzeń są czterocyfrowymi liczbami w schemacie 46*xx* (większość) i 47*xx* (mniejszość).

Logi Windows

Zmiany polityki

Windows loguje także zdarzenia dotyczące zmiany samej polityki audytu. W tym wypadku są to dokładnie dwa typu zdarzeń. Pierwszy ma identyfikator 4719 i dotyczy zmiany ustawień audytu, a drugi ma identyfikator 1102 i dotyczy wyczyszczenia zawartości logów bezpieczeństwa.

Logi Windows

Inne

Windows rejestruje też domyślnie zdarzenia dotyczące usług i umieszcza je w dzienniku systemowym (System Logs). Można także włączyć dla nich zaawansowany audyt, który będzie dodawał informacje o tych zdarzeniach do dziennika bezpieczeństwa (Security Log). Ponadto prowadzony jest osobny dziennik dla zdarzeń dotyczących sieci WLAN oraz rejestrowane są zdarzenia pochodzące z *Windows Filtering Platform* i oprogramowania antywirusowego *Windows Defender*. Dodatkowo istnieje możliwość włączenia śledzenia procesów, użytkowania aplikacji, a także wykorzystania powłoki *PowerShell*. Warto także rozważyć użycie darmowego narzędzia do rejestrowania zdarzeń o nazwie *Sysmon*. Zbiera on więcej danych o zdarzeniach niż robią to standardowe mechanizmy logowania.

Logi Linuksa

Linux, w przeciwieństwie do systemu Windows, przechowuje większość danych o zdarzeniach w plikach tekstowych, co ułatwia ich analizę przy pomocy narzędzi dostępnych ▸ w powłokach systemowych. Przykładowo, można użyć narzędzia `grep` (lub jego zamiennika) do wyszukiwania wzorców w logach. Z kolei narzędzia takie jak `tail` i `less` umożliwiają obserwowanie zmian w dziennikach w czasie rzeczywistym. Domyślnie większość plików dzienników jest zgromadzona w katalogu `/var/log/`. Tradycyjnie najważniejszą usługą w systemie Linux (i wielu pokrewnych należących do rodziny Uniksa) odpowiedzialną za logowanie zdarzeń jest demon `syslog`. W przypadku dystrybucji Linuksa bazujących na Red Hat, zdarzenia są zapisywane przez `syslog` do pliku `/var/log/messages`. Natomiast dystrybucje bazujące na Debianie umieszczają te informacje w pliku `/var/log/syslog`.

Logi Linuksa

Logi jądra

Jądro systemu ma swój własny bufor cykliczny (ang. *ring buffer*) w którym umieszcza informacje dotyczące zdarzeń związanych z jego działaniem. Zawartość tego bufora można wyświetlić na ekranie przy pomocy programu `dmesg`. Nowsze wersje tego programu kolorują wyświetlany tekst, co ułatwia odnajdywanie istotnych informacji. Ponadto posiadają one opcje, które umożliwiają śledzenie na bieżąco zmian zawartości bufora (`-w`) pomiar czasu między kolejnymi zdarzeniami (`-d`) wyświetlenie czasu zdarzenia w formie czytelnej dla człowieka oraz uproszczenie nawigowania po wyświetlonym tekście (`-H`). Istnieją również dwie opcje, które umożliwiają wyczyszczenie bufora cyklicznego, ale wymagają uprawnień użytkownika `root` (opcja `-c`, czyli wyświetlenie bieżącej zawartości i wyczyszczenie bufora oraz `-C`, tylko wyczyszczenie).

Logi Linuksa

Logi jądra

Aby dodatkowo chronić informacje zawarte w buforze cyklicznym można wymagać, aby polecenie `dmesg` było wykonywane tylko przez uprawnionych użytkowników. Wymaga to zmiany wartości parametru `kernel.dmesg_restrict` na 1. Parametr ten znajduje się w pliku `/etc/sysctl.d/10-kernel-hardening.conf`. Nowsze wersje dystrybucji Debian i Ubuntu nadają taką wartość temu parametrowi domyślnie.
Również oprogramowanie `syslog` pobiera informacje z bufora cyklicznego jądra i w zależności od konfiguracji, wypisuje je na konsoli lub umieszcza w plikach dziennika. Zazwyczaj są to pliki `boot.log` i `kern.log` w katalogu `/var/log`.

Logi Linuksa

Logi `systemd`

Proces **`systemd`** jest managerem systemu i usług w Linuksie, który zastąpił proces **`initd`** znany z wersji System V Uniksa. Posiada on osobny ▸ mechanizm, nazwany **`journal`**, który odpowiedzialny jest za rejestrowanie zdarzeń dotyczących usług, urządzeń, gniazd i innych elementów systemu zarządzanych przez **`systemd`**. W zasadzie są to dane audytowe pochodzące z całego systemu, które **`journal`** umieszcza w jednym miejscu, co ułatwia ich analizę. Niestety są one zapisywane w postaci binarnej i w związku z tym wymagają specjalnego narzędzia do ich przeglądania. Głównym komponentem tego mechanizmu jest demon **`systemd-journald`**. Jego zachowanie jest konfigurowane przy pomocy pliku **`/etc/systemd/journald.conf`**. Dane o zdarzeniach są zapisywane najpierw w katalogu **`/run/log/journal/`**, a dopiero potem trafiają do **`/var/log/journal/`**, choć można tak skonfigurować **`journal`**, aby były zapisywane tylko w pamięci ulotnej.

Logi Linuksa

Logi `systemd`

Głównym narzędziem do przeglądania dzienników `journal` jest polecenie powłoki `journalctl`. Uruchomienie tego narzędzia bez opcji rozpocznie wyświetlanie na ekranie, w formie czytelnej dla człowieka, zawartości dziennika zdarzeń, począwszy od chwili uruchomienia systemu. Tekst jest kolorowany i można w nim nawigować tak jak przy użyciu narzędzia `less`. Opcja `-f` pozwala śledzić zmianę treści pliku z logami na bieżąco. Z kolei opcje `--since` i `--until` pozwalają określić z jakiego okresu zdarzenia będą wyświetlone. Jako argument dla tego polecenia można też podać nazwę pliku wykonywalnego i ono znajdzie informacje o zdarzeniach związanych z tym programem. Opcja `-u` pozwala z kolei wyszukać informacje o zachowaniu konkretnej usługi, a dokładniej jednostki `systemd`. Opcja `-k` powoduje wyświetlenie komunikatów jądra, a `-e` przejście na koniec dziennika zdarzeń. Opcja `-x` generuje dodatkowe informacje o błędach. Są także inne opcje, które opisane są np. w podręczniku `man`.

Logi Linuksa

Logi `syslog`

Mechanizm `syslog` jest domyślnym mechanizmem logowania w Linuksie i wielu innych systemach operacyjnych wywodzących się z Uniksa. Oferuje on szereg przydatnych ▸ możliwości. Przykładowo, oprócz wspomnianego wcześniej pliku `syslog` lub `messages`, pozwala aplikacjom tworzyć ich własne dzienniki w katalogu `/var/log/`. Może też być tak skonfigurowany, aby rozdzielał poszczególne dane audytowe na osobne pliki. Przykładowo komunikaty dotyczące uwierzytelniania użytkowników w systemie są zapisywane w pliku `auth.log`. Istnieje wiele implementacji tego komponentu. Przykładowo, dystrybucja Ubuntu używa `rsyslogd`, a konfiguracja tej wersji jest zapisana w pliku `/etc/rsyslog.conf` oraz katalogu `/etc/rsyslog.d/`. Aplikacje mogą przekazywać informację o zdarzeniach za pomocą specjalnego API, w skład którego wchodzi gniazdo `/dev/log`.

Logi Linuksa

Logi `syslog`

Syslog dysponuje własnym protokołem, opisanym w dokumencie RFC 5452. Nie tylko definiuje on strukturę informacji o zdarzeniach, ale również umożliwia przesłanie logów do zewnętrznych systemów typu SIEM, celem ich dalszej analizy. Dodatkowo informacje te mogą być przesyłane w sposób zaszyfrowany.

Polecenie `last`

Polecenie `last` wypisuje na ekranie informacje o ostatnich logowaniach do systemu, przy czym najnowsze dane znajdują się u góry ekranu. Zatem wygodniej jest go używać w potoku np. z `less`. Plik dziennika, z którego to narzędzie korzysta to (częściej) `/var/log/wtmp` lub (rzadziej) `/var/log/btmp`. W systemie mogą występować oba te pliki, ale również oba mają format binarny, zatem nie można przeglądać ich zawartości przy pomocy narzędzi do przetwarzania tekstu.

Logi Linux

Obsługa logów

Ponieważ pliki logów tworzone przez `syslog` mogą szybko urosnąć do dużych rozmiarów, to większość dystrybucji Linuksa ma zainstalowanego specjalnego demona o nazwie `logrotate`, który odpowiedzialny jest za ich kompresję, usuwanie a nawet wysyłanie przez e-mail tych plików. To, co dokładnie to oprogramowanie zrobi z logami można skonfigurować. Plikiem konfiguracyjnym dla tego narzędzia jest `/etc/logrotate.conf`, ale reguły dla poszczególnych dzienników programów korzystających z `syslog` są zapisane w katalogu `/etc/logrotate.d/`.

Warto także rozważyć zainstalowanie narzędzia `logcheck`, które działając jako demon będzie monitorowało dzienniki i wykrywało wskazane nieprawidłowości. Zachowanie tego narzędzia można skonfigurować dokonując odpowiednich zmian w plikach znajdujących się w katalogu `/etc/logcheck/`.

Logi Linux

Odzyskiwanie skasowanych logów

Dla systemu Linux dostępne jest oprogramowanie stworzone na potrzeby informatyki śledczej o nazwie *X-Ways Forensic*. Potrafi ono m.in. odzyskać z obrazu partycji skasowane pliki dzienników zdarzeń [1]. Całkowite odzyskanie jest możliwe tylko wtedy, gdy obraz został zrobiony w krótkim czasie po usunięciu plików, kiedy system operacyjny nie przydzielił jeszcze bloków danych do nich należących innym plikom. Jeśli jednak tak się już stało, to dzięki opisywanemu narzędziu uda się być może odzyskać częściowo zawartość dzienników.

Literatura

 Andrzej Ziaja. *Praktyczna analiza powłamaniowa.* Aplikacja webowa w środowisku Linux. Polskie Wydawnictwa Naukowe (PWN), Warszawa, 2017.

Pytania

?

KONIEC

Dziękuję Państwu za uwagę!