STUDIA INFORMATICA 2011
Volume 32 Number 2B (97)

Paweł JAWORSKI
Politechnika Śląska, Instytut Informatyki

AUDYT SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA W FIRMIE Z ZASTOSOWANIEM OTWARTEGO OPROGRAMOWANIA OPEN-AUDIT

Streszczenie. Na rynku dostępnych jest wiele programów, które wykonują audyt sprzętu komputerowego oraz oprogramowania. Są to oprogramowania płatne. Open-AudIT jest oprogramowaniem bezpłatnym, udostępnianym na podstawie licencji GNU. Funkcjonalność przedmiotowej aplikacji nie odbiega zakresem audytowanych obszarów od rozwiązań komercyjnych, a niejednokrotnie pozwala na zbadanie w szerszym zakresie sprzętu i oprogramowania należących do organizacji.

Słowa kluczowe: audyt sprzętu komputerowego, audyt oprogramowania, WMI, HAL, Nmap

AUDIT HARDWARE AND SOFTWARE IN THE COMPANY WITH THE USE OF OPEN-AUDIT SOFTWARE

Summary. On the market there are many programs which perform audits of computer hardware and software. These are payable software. Open-AudIT is free software released under the GNU License. The functionality of the application, when it comes to the range of audited areas, does not differ from commercial solutions, and often allows to explore more widely the hardware and software owned by the organization.

Keywords: hardware audit, software audit, WMI, HAL, Nmap

1. Wstęp

Zasoby informatyczne organizacji stanowią znaczną część jej majątku. W celu jak najlepszego gospodarowania poszczególnymi elementami tych zasobów, niezbędne jest posiadanie odpowiednich narzędzi służących do ewidencjonowania, sprawdzenia stopnia ich wykorzy-

stania. Niejednokrotnie okazuje się, że organizacja dokonuje nowych zakupów infrastruktury informatycznej, takich jak: oprogramowanie stanowiskowe, oprogramowanie specjalistyczne, mimo że posiada takie aplikacje, ale nie ma informacji, czy są one wykorzystywane na poszczególnych stanowiskach.

Kolejnym powodem, który determinuje tworzenie szczegółowej ewidencji sprzętu i oprogramowania w organizacji, są wymogi prawne. Zgodnie z Ustawą o prawie autorskim i prawach pokrewnych (DzU z 2006 r. nr 90, poz. 631 z późn. zm.), dokonując zakupu licencji na oprogramowanie można go wykorzystywać na ograniczonej liczbie stanowisk (determinują to zapisy w umowie licencyjnej). Im większa organizacja, tym trudniej jest, bez odpowiedniego narzędzia, ewidencjonować zainstalowane oprogramowanie na poszczególnych stacjach roboczych, gdzie niejednokrotnie użytkownicy posiadają prawa umożliwiające instalację nowych aplikacji.

W ofercie firm można znaleźć wiele systemów prostych lub bardziej złożonych, umożliwiających wykonywanie zarówno ewidencji posiadanych zasobów informatycznych, jak i ich audyt. Są to jednak rozwiązania płatne, a wysokość opłat licencyjnych za ich użytkowanie jest ściśle powiązana z liczbą audytowanych stacji roboczych.

Jest również dostępne rozwiązanie bezpłatne, udostępniane na podstawie licencji GNU (General Public License wersja 2), opublikowanej przez Free Software Foundation. Jest to oprogramowanie Open-AudIT.

Open-AudIT jest następcą Winventory, podobnego projektu typu open source, z którego pochodzi kod bazowy. Jednak w porównaniu ze swoim poprzednikiem, Open-AudIT wykorzystuje nowe mechanizmy w celu dodawania danych do bazy [1].

2. Budowa aplikacji Open-AudIT

2.1. Serwer Open-AudIT

Aplikacja, aby mogła prawidłowo działać, musi być zainstalowana na serwerze, który jest wyposażony w serwer bazy danych MySQL oraz serwer WWW, obsługujący PHP.

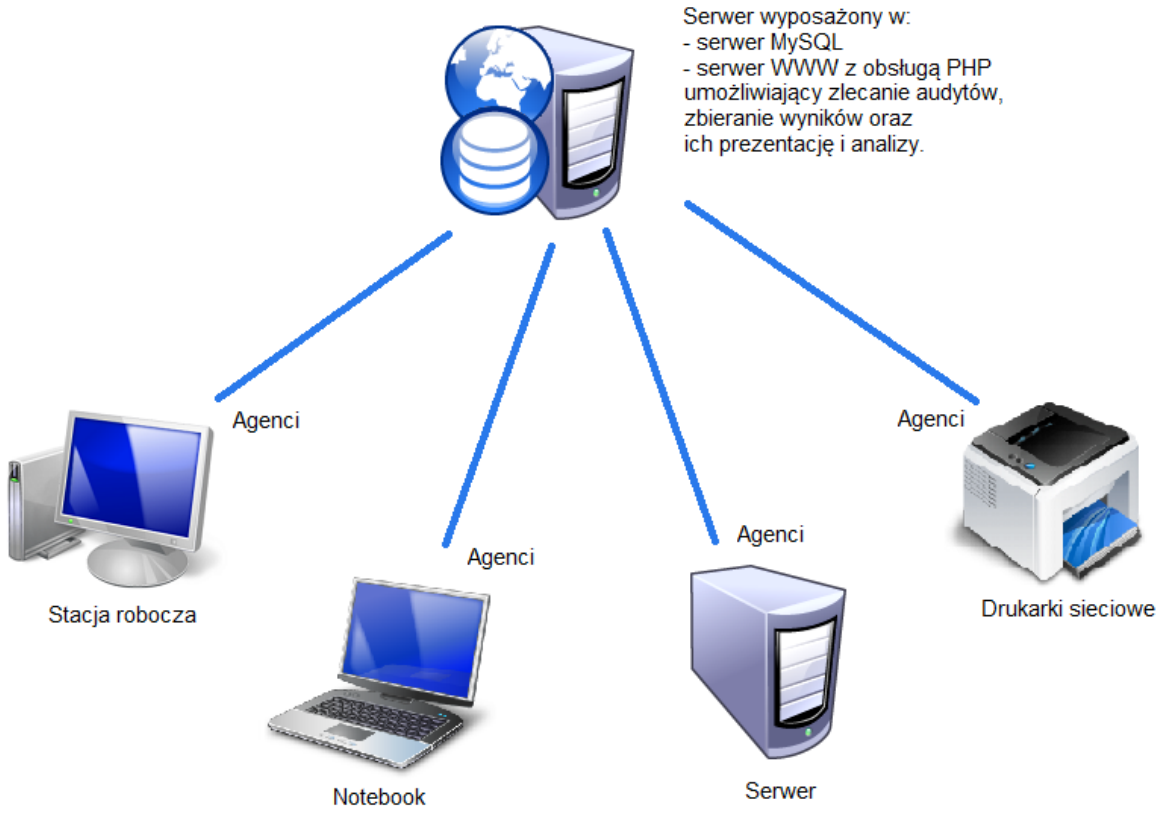
Testując aplikację Open-AudIT, zostały zbudowane dwa środowiska:

- testowe, zbudowane z 4 urządzeń, nazywane w dalszej części – środowisko 1,
- produkcyjne, zbudowane na bazie dużej jednostki administracji publicznej, gdzie zostało objętych audytem około 500 urządzeń, nazywane w dalszej części – środowisko 2.

Środowisko 1 składa się z serwera zbudowanego na bazie MS Windows 7 Professional 32-bit z zainstalowanym oprogramowaniem WAMPSEVER 2.1, w którego skład wchodzą

serwery Apache, PHP, MySQL. Badane urządzenia: 2 notebooki oraz 1 netbook. Środowisko 1 nie posiada domeny.

Środowisko 2 składa się z serwera zbudowanego na bazie serwera Linux z zainstalowanymi serwerami Apache, PHP i MySQL. Badane urządzenia: serwery, komputery stacjonarne, notebooki, drukarki sieciowe. Środowisko 2 posiada domenę.



Rys. 1. Elementy systemu Open-AudIT
Fig. 1. Elements of the system Open-AudIT

Na rys. 1 przedstawiono strukturę, jaką tworzy system Open-AudIT. Dla małych sieci wystarczające jest, aby serwer działał na bazie systemu Windows. Do większych rozwiązań zasadne jest zastosowanie serwera linuxowego lub takie zaplanowanie wykonywania audytu, aby stanowiska komputerowe nie były audytowane w jednym czasie.

Agenci mogą być uruchamiani lokalnie lub zdalnie, wykonując inwentaryzację zarówno stacji roboczych, jak i urządzeń sieciowych. Agenci po wykonaniu audytu przekazują dane do serwera za pomocą metody POST.

2.2. Mechanizm audytu

Open-AudIT umożliwia inwentaryzację stanowisk komputerowych i serwerów opartych na systemach MS Windows oraz Linux. Ponadto, dysponuje narzędziami umożliwiającymi

skanowanie sieci komputerowej i ewidencję urządzeń podłączonych do niej, takich jak drukarki sieciowe.

2.2.1. Audyt systemów opartych na MS Windows

Stanowiska komputerowe oparte na systemie MS Windows są audytowane na podstawie Windows Management Instrumentation (WMI) oraz Windows Script Host (WSH). Starsze systemy, takie jak Windows 95 i Windows NT, mogą mieć problemy z audytem, gdyż WSH należy doinstalować ręcznie [1].

WSH jest zestawem komponentów systemu, dzięki którym możliwe jest uruchamianie i działanie skryptów VBScript. Mechanizm ten jest przeznaczony do wyeliminowania jednego z głównych ograniczeń na platformach Windows w zakresie automatyzacji obsługi rejestru lub uzyskania informacji na temat systemu plików [2].

Usługa WMI firmy Microsoft to implementacja WBEM (Web Based Enterprise Management Initiative), inicjatywy ustanowienia standardów uzyskiwania dostępu do informacji o zarządzaniu oraz ich udostępniania w sieci przedsiębiorstwa. Usługa WMI zapewnia zintegrowaną obsługę modelu danych CIM (Common Information Model), który opisuje obiekty istniejące w środowisku zarządzania [3].

Usługa WMI zawiera repozytorium obiektów, które jest bazą danych definicji obiektów oraz menedżera obiektów WMI, obsługującego zbieranie obiektów i operacje przeprowadzane na nich w repozytorium, a także gromadzącego informacje od dostawców WMI. Dostawcy WMI pełnią rolę pośredników pomiędzy usługą WMI a składnikami systemu operacyjnego, aplikacjami i innymi systemami. Na przykład dostawca rejestru pobiera dane z rejestru, a dostawca usługi SNMP dostarcza dane i zdarzenia z urządzeń SNMP. Dostawcy zapewniają informacje dotyczące swoich składników oraz metod ich obsługi, właściwości, które można ustawiać, a także zdarzeń, które mogą alarmować o zmianach w składnikach [3].

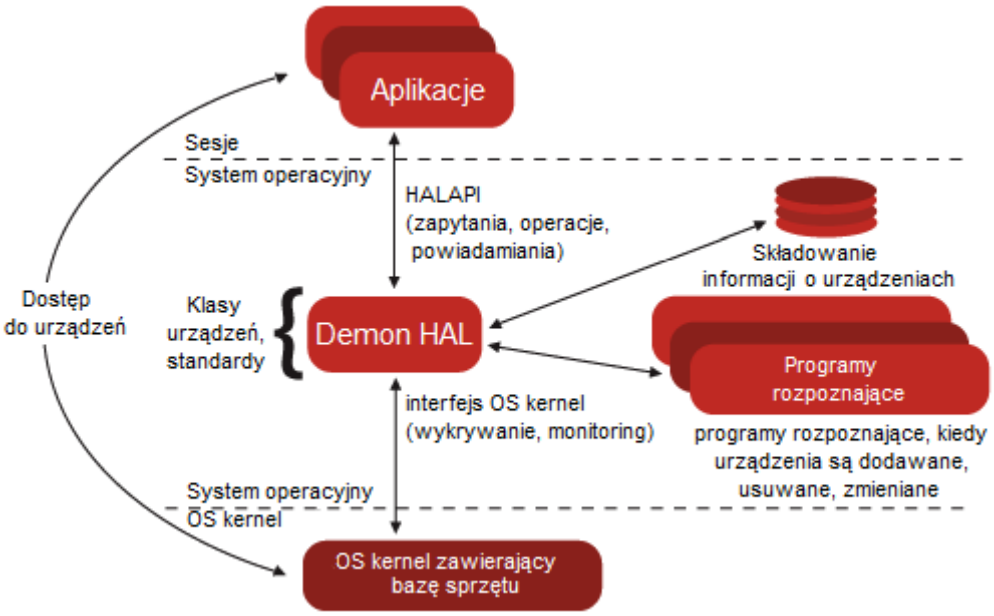
Usługa WMI może wspomagać narzędzia do zarządzania komputerami. WMI może być także używana z systemami programowania lub skryptów (np. WSH) w celu pobierania szczegółów konfiguracji większości elementów systemów komputerowych, w tym również aplikacji [3].

2.2.2. Audyt stanowisk z systemem Linux

Na stanowiskach komputerowych, na których zainstalowany jest system Linux (OpenAudIT obsługuje dystrybucje Fedora i Ubuntu), inwentaryzacja jest wykonywana z pomocą bibliotek i sterowników Hardware Abstraction Layer (HAL).

Standardowo aplikacje rozpoznają sprzęt, komunikując się bezpośrednio z jądrem systemu (rys. 2) [4]. Kernel utrzymuje listę urządzeń podłączonych do systemu. Jest to żmudny i niedokładny proces, ponieważ czasami jądro nie wie wszystkiego o danym urządzeniu. Na

przykład, niektóre aparaty cyfrowe i przenośne odtwarzacze muzyki są rozpoznawane jako kolejny dysk twardy w interfejsie użytkownika [4].



Rys. 2. Opis działania HAL
Fig. 2. Functioning of the HAL

HAL umożliwia uzyskanie wszystkich interesujących informacji na temat niektórych klas sprzętu w łatwo dostępnym formacie, dobrze zdefiniowanym. Kiedy nowe urządzenie jest dodawane do systemu, na magistrali komunikatów systemowych, nadawany jest sygnał, szczegółowo określający, jakiego rodzaju urządzenia dodano. Każda aplikacja może podłączyć się do magistrali komunikatów w celu wykrycia sprzętu [4, 5].

Wobec powyższego, na poziomie aplikacji można, wykorzystując HAL, dokonać inspekcji sprzętu. HAL również umożliwia gromadzenie informacji w zakresie oprogramowania działającego na badanym komputerze.

Open-AudIT do wykonania inwentaryzacji posługuje się skryptem audit_linux.sh, znajdującym się w katalogu scripts. Skrypt ten należy uruchomić na każdym stanowisku z zainstalowanym systemem Linux.

2.2.3. Audyt urządzeń sieciowych

Do wykonywania audytu urządzeń sieciowych służy narzędzie Network Mapper (Nmap). Jest to darmowe oprogramowanie udostępniane na zasadach licencji GNU General Public License. Nmap jest narzędziem do eksploracji sieci i audytów bezpieczeństwa. Wykorzystuje pakiety IP, sprawdzając, które adresy są dostępne w sieci oraz jakie usługi oferuje dane urządzenie w obrębie sieci (nazwa aplikacji i wersja). Implementuje wiele różnych technik testowania portów TCP, w tym niestandardowe podejścia wynikające ze specyfiki implementacji stosów sieciowych, które potencjalnie mogą omijać zapory sieciowe lub platformy Intrusion

Detection System. Dodatkowo Nmap posiada możliwość identyfikacji systemów operacyjnych na skanowanych hostach. Został zaprojektowany do szybkiego skanowania dużych sieci, ale działa dobrze w stosunku do pojedynczych adresów [6].

Open-AudIT wykorzystuje Nmap. Za pomocą skryptu nmap.vbs, znajdującego się w katalogu scripts, zbiera informacje dotyczące zainstalowanych urządzeń sieciowych, takich jak np. drukarki sieciowe [1].

2.3. Metody wykonywania audytu

Aplikacja umożliwia trzy sposoby przeprowadzania audytu infrastruktury informatycznej:

- ręczny – za pomocą skryptu uruchamianego na każdej stacji roboczej,
- automatyczny – konfigurowanego z poziomu warstwy prezentacyjnej Open-AudIT,
- jako skrypt uruchamiany na każdym stanowisku roboczym będącym w domenie.

Każda z tych metod wymaga skonfigurowania odpowiednich plików.

Ręczne wywoływanie skryptu polega na zalogowaniu się na stronę lokalnego serwera Open-AudIT i wywołania polecenia Admin -> AuditMyMachine. Po uruchomieniu tej opcji zostanie zapisany na dysk lokalny odpowiednio przygotowany plik vbs, umożliwiający inwentaryzację tego stanowiska pracy. Uruchomienie pliku vbs spowoduje utworzenie pliku konfiguracyjnego oraz wykonanie audytu. Wyniki zostają wysłane do serwera Open-AudIT.

Druga z metod automatycznego przeprowadzania audytu wymaga zarówno przygotowania stanowisk poddawanych inspekcji, jak i odpowiedniego skonfigurowania skryptów. W celu wykonania zdalnej inspekcji w systemach Windows niezbędne jest włączenie na firewall stanowiska pracy zdalnego administrowania. Można posłużyć się skryptem firewall_enable-.vbs, znajdującym się w katalogu scripts. Ponadto, w warstwie prezentacyjnej Open-AudIT należy przygotować konfigurację audytu oraz cykl jej wykonywania za pomocą poleceń dostępnych w Audits -> Manage Audits.

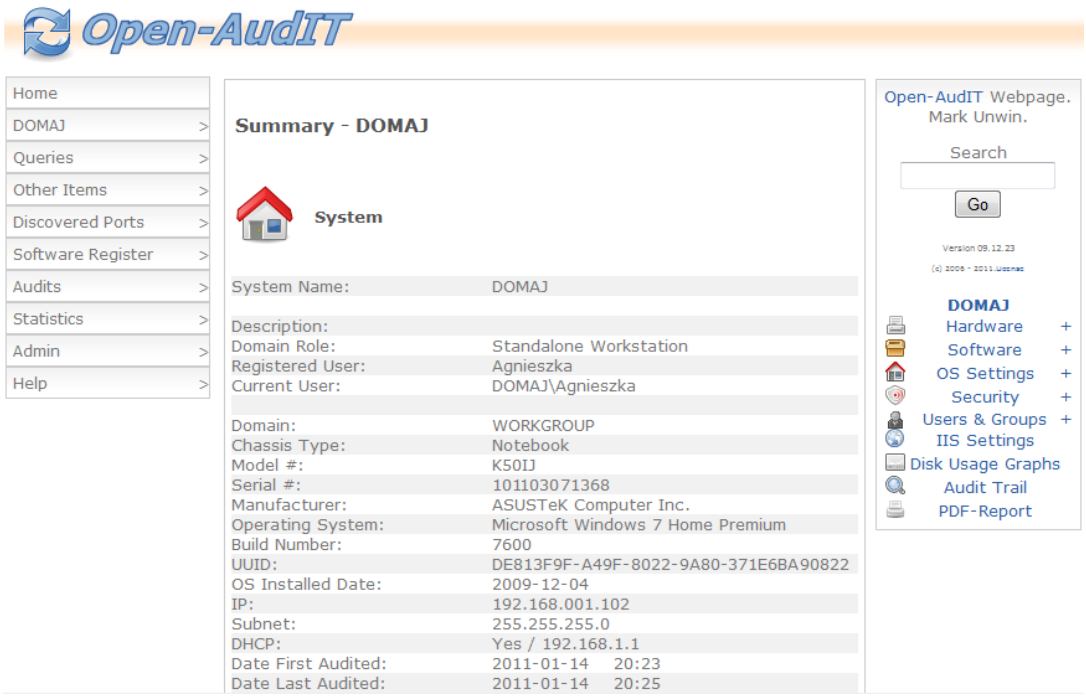
Najbardziej polecanym rozwiązaniem w przypadku dużej infrastruktury informatycznej jest uruchamianie skryptów inwentaryzujących sprzęt i oprogramowanie w środowisku domeny. Należy zaznaczyć, iż niezbędne jest posiadanie uprawnienia do kontroli systemów zdalnych. Trzeba odpowiednio przygotować plik audit.config.xml, znajdujący się w katalogu scripts. Audyty należy wykonywać w ustalonych cyklach czasowych. W ramach przeprowadzanych testów – środowisko 2 – skrypt kontroli został połączony ze skryptem logowania do domeny, tak aby za każdym razem, gdy użytkownik loguje się do domeny był wykonywany audyt. Takie rozwiązanie umożliwia rejestrację w Open-AudIT, kiedy i jaki użytkownik logował się na danej stacji roboczej.

2.4. Warstwa prezentacyjna Open-AudIT

Open-AudIT dysponuje bardzo rozbudowaną warstwą prezentacyjną. Na stronie głównej można wyświetlać bieżące informacje o takich zagrożeniach, jak np:

- partycje, w których ilość wolnego miejsca wynosi xxx MB (xxx jest definiowane),
- nowe systemy audytowane w okresie ostatnich xxx dni (xxx jest definiowana),
- inne wykryte urządzenia w okresie ostatnich xxx dni (xxx jest definiowana),
- nowe oprogramowanie wykryte w ciągu ostatnich xxx dni (xxx jest definiowana).

To tylko kilka przykładów, które umożliwiają śledzenie zmian w audytowanej infrastrukturze informatycznej. Open-AudIT bardzo szczegółowo zbiera informacje o poszczególnych stacjach roboczych. Rysunek 3. przedstawia przykładowe dane z jednej z nich.



Rys. 3. Zrzut ekranu Open-AudIT
Fig. 3. Screenshots Open-AudIT

Warstwa prezentacyjna Open-AudIT zawiera również gotowe zestawienia, które są pomocne w bieżącej pracy administratora infrastruktury informatycznej jednostki. Są to zestawienia dotyczące między innymi statusów programów antywirusowych na poszczególnych stacjach roboczych, mapowanych zasobów, utworzonych lokalnych kont administratorów.

Ponadto, Open-AudIT zawiera sekcje statystyk, umożliwiającą wykonanie zestawień zbiorczych w zakresie posiadanych: systemów operacyjnych, przeglądarek internetowych i ich wersji, pamięci RAM, dysków twardych, typów procesora.

Wykorzystując narzędzie Nmap, warstwa prezentacyjna Open-AudIT prezentuje zebrane wyniki. Są to informacje o otwartych portach w urządzeniach oraz na stacjach roboczych.

Analizując zainstalowane oprogramowanie na stacjach roboczych Open-AudIT, umożliwia prowadzenie ewidencji posiadanych licencjach i wykonania zestawienia ich wykorzystania oraz braków. Zaletą tego modułu jest możliwość wskazania, że dane oprogramowanie jest darmowe i nie wymaga posiadania stosownych licencji.

Z uwagi na to, że Open-AudIT jest otwartym oprogramowaniem, można go dowolnie dostosować do własnych potrzeb. Przykładowo, w standardowej wersji instalacyjnej brak jest wyboru polskiego menu. Jednak wersję językową można samodzielnie zmienić – wystarczy przetłumaczyć plik en.inc znajdujący się w katalogu „openaudit\lang" i nadać mu nazwę, np. pl.inc. Wówczas w ustawieniach Open-AudIT pojawi się wersja językowa „pl".

3. Podsumowanie

Open-AudIT jest darmową aplikacją, która stanowi alternatywę dla rozwiązań biznesowych. Umożliwia przeprowadzenie audytu całej infrastruktury jednostki. Mimo braku szczegółowej dokumentacji, informacje zawarte na stronie http://www.open-audit.org/, a w szczególności na forum, umożliwiają odpowiednie przygotowanie plików konfiguracyjnych w celu wykonywania audytów zarówno dla małych, jak również dużych organizacji. Zaletą Open-AudIT jest możliwość rozbudowy oprogramowania i dostosowania go do własnych potrzeb.

Ponadto, zbieranie bardzo szczegółowych danych o całej infrastrukturze informatycznej jednostki umożliwia wykrycie słabych jej punktów i daje administratorowi możliwość wykonania odpowiednich działań prewencyjnych.

BIBLIOGRAFIA

1. Projekt: Open-AudIT, http://www.open-audit.org/.
2. Lomax P., Childs M., Petrusha R.: VBScript in a nutshell. O'Reilly, USA 2003.
3. Windows Server TechCenter, http://technet.microsoft.com/pl-pl/library/cc736575(WS.10)-.aspx.
4. Zeuthen D.: Desktop and Hardware Configuration. Red Hat Magazine, January 2005.
5. Projekt: freedesktop.org, http://freedesktop.org/wiki/Software/hal/.
6. Projekt: Network Mapper, http://nmap.org/.

Recenzenci: Dr inż. Adrian Kapczyński
Prof. dr hab. inż. Bolesław Pochopień

Wpłynęło do Redakcji 31 stycznia 2011 r.

Abstract

On the market there are many programs that offer performing a hardware and software audit. These are payable software. Open-AudIT is software released under the GNU (General Public License Version 2) and published by the Free Software Foundation. The functionality of the application, when it comes to the range of audited areas, does not differ from commercial solutions, and often allows to explore more widely the hardware and software owned by the organization.

Open-Audit allows you to perform an audit on PCs running MS Windows and Linux. In addition, it can be used to inventory of network devices such as network printers.

Adres

Paweł JAWORSKI: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16,
44-100 Gliwice, Polska, paolojaw@gmail.com