

VIII Konferencja PLOUG
Kościelisko
Październik 2002

Narzędzia do testowania bezpieczeństwa Oracle

Wojciech Dworakowski

wojtekd@ipsec.pl

Po co testować bezpieczeństwo Oracle

Niewielu ludzi myśli o bazach danych gdy mówi się o „bezpieczeństwie IT”. Ale gdy zadamy sobie pytanie: „Gdzie są przechowywane kluczowe zasoby naszej organizacji?” od razu kojarzą się nam serwery bazodanowe. Utarło się że serwery te są elementem infrastruktury wewnętrznej, więc nie zwraca się uwagi na ich bezpieczeństwo. Są umieszczone za serwerami aplikacyjnymi i serwerami www, które stanowią interfejsy do danych zgromadzonych w bazach. Większość administratorów myśli o bezpieczeństwie serwerów bazodanowych wyłącznie w kontekście ustawienia odpowiednich reguł filtrowania na firewallach. Jednak często okazuje się to nieskuteczne, gdyż dostęp do baz i tak jest realizowany przez interfejsy webowe lub aplikacyjne. Poza tym większość ataków na systemy bazodanowe to ataki operujące na wysokich warstwach modelu OSI, zaś firewalle przeważnie filtrują ruch na trzeciej i czwartej warstwie OSI.

Weźmy pod uwagę następujący przykład:

Dysponujemy serwerem aplikacyjnym Oracle 9iAS i chcemy udostępnić na nim aplikację służącą do składania zamówień przez Internet. Prawdopodobnie firewall zostanie skonfigurowany w ten sposób, że będzie blokować cały ruch do tego serwera z wyjątkiem ruchu na port 80 TCP (lub inny na którym działa serwer aplikacji). Oczywiście taka konfiguracja nie chroni serwera przed atakami na moduły serwera www Apache, które w standardowej wersji zawierają błędy pozwalające nawet na zdalne opanowanie serwera.

Powyższy przykład jest dosyć trywialny, jednak dobrze ilustruje nieskuteczność standardowych mechanizmów ochrony.

Należy pamiętać że blisko 80% incydentów związanych z atakami na systemy IT pochodzi z wnętrza organizacji które są ofiarami tych wypadków.

Same oprogramowanie DBMS nie gwarantuje nam dostatecznego poziomu bezpieczeństwa. Argumenty potwierdzające tą tezę przedstawiłem w poprzednim wykładzie. W takim razie – elementem każdego projektu powinno być zapewnienie odpowiedniego poziomu bezpieczeństwa również dla systemów bazodanowych.

Jak to zrobić?

Utrzymanie pożądanego poziomu bezpieczeństwa jest procesem ciągłym. Polega ono na ciągłym testowaniu bezpieczeństwa i wprowadzaniu poprawek. Przed wdrożeniem projektu wskazane jest przeprowadzenie testu bezpieczeństwa przez doświadczony i zaawansowany zespół z zewnątrz, w formie testu penetracyjnego (który polega na kontrolowanych próbach włamania) lub audytu (który polega na kompleksowym sprawdzeniu procedur i konfiguracji systemów). Rezultatem takiego testu jest raport, który zawiera opis znalezionych przez zespół zagrożeń. Potem należy wprowadzić niezbędne poprawki zmierzające do wyeliminowania wykrytych zagrożeń i już można w miarę spokojnie przystąpić do wdrażania projektu.

Jak jednak dbać o utrzymanie założonego poziomu bezpieczeństwa? Codziennie są ujawniane nowe rodzaje zagrożeń. Konfiguracja serwerów również nie pozostaje statyczna: administratorzy wprowadzają zmiany poprawiające działanie serwisów, programiści poprawiają swoje aplikacje. Paradoksalnie - nawet wgrywanie poprawek przygotowanych przez producenta może wprowadzać nowe zagrożenia lub przywracać standardową konfigurację części modułów.

Częste przeprowadzanie testów penetracyjnych i audytów okazuje się nieefektywne czasowo i ekonomicznie. Z pomocą przychodzą tu narzędzia do testowania bezpieczeństwa systemów bazodanowych. Narzędzia te naśladują działania audytorów, jednak oczywiście nie dysponują właściwą człowiekowi inteligencją i dociekliwością

Funkcje narzędzi automatycznych

W tej chwili na rynku jest dostępnych kilka narzędzi nadających się do okresowego, zautomatyzowanego testowania bezpieczeństwa systemów Oracle. Poniżej przedstawię najczęściej realizowane przez nie funkcje. Dalej postaram się krótko przybliżyć kilka skanerów bezpieczeństwa Oracle, z którymi miałem okazję się zapoznać.

Inwentaryzacja aplikacji

Większość skanerów jest w stanie przeszukiwać zadany zakres adresów IP w poszukiwaniu serwerów bazodanowych. Potrafią także w obrębie jednego serwera wyszukać aplikacje i serwisy za pośrednictwem których można dostać się do danych. W przypadku Oracle jest to stosunkowo proste – wystarczy wysłać odpowiednie żądanie TNS do listenera. Informacja ta bywa też zdobywana w wyniku sprawdzania otwartych portów i sprawdzenia serwisów, które na nich nasłuchują.

„Testy penetracyjne”

A raczej ich symulacja, gdyż testy wykonane skanerem automatycznym nie mogą być uważane za testy penetracyjne. Jednak większość dostawców oprogramowania testującego używa tego terminu. Prawidłową nazwą byłyby: Ataki z zewnątrz.

Ta funkcjonalność obejmuje ustalenie na jakie zagrożenia jest podatny system bazodanowy, gdy intruz działa z zewnątrz i nie posiada żadnych przywilejów. Skanery robią to wykonując szereg testów poprzez sieć i porównując ich rezultaty z bazą ataków jaką dysponują.

Audyty konfiguracji

Niektóre ze skanerów posiadają również funkcje audytu (znowu – nazwa raczej umowna). Skaner dysponując kontem administracyjnym (w przypadku skanerów dla Oracle wymagane są uprawnienia użytkownika SYS lub SYSTEM) i odpowiednim hasłem, loguje się zdalnie do DBMS-a i sprawdza jego konfigurację. Poszczególne produkty różnią się między sobą rodzajem i dokładnością wykonywanych testów.

Z reguły udostępniają one możliwość sprawdzania haseł przez próby łamania metodą słownikową, sprawdzanie bazy użytkowników, inwentaryzację uprawnień, wychwytywanie użytkowników o bardzo wysokich uprawnieniach. Posiadają też możliwości analizowania informacji w tabelach systemowych, a co za tym idzie możliwość szczegółowego audytu konfiguracji.

Część narzędzi dysponując kontem w systemie operacyjnym, jest też w stanie dokonać głębszego przeglądu konfiguracji przez zdalne zalogowanie się do systemu operacyjnego i sprawdzenie plików konfiguracyjnych oraz działających procesów.

Współczesne skanery bezpieczeństwa DBMS działają całkowicie zdalnie i nie wymagają instalacji żadnego dodatkowego oprogramowania na serwerze Oracle. Jedynym warunkiem jest udostępnienie im możliwości zdalnego uwierzytelnienia na konto z uprawnieniami administracyjnymi.

Raportowanie

Z reguły skanery posiadają szerokie możliwości sporządzania raportów. Warto zauważyć, że w dużych systemach, skaner bezpieczeństwa DBMS można wykorzystać również do dokumentowania systemu wykorzystując funkcje inwentaryzacji aplikacji, inwentaryzacji konfiguracji oraz inwentaryzacji użytkowników i uprawnień.

Przydatną funkcją jest możliwość porównania zmian jakie zaszły na serwerze DBMS od ostatniego skanu.

Czym kierować się przy wyborze narzędzia?

Baza sygnatur zagrożeń

Sercem każdego skanera bezpieczeństwa jest baza zagrożeń. Skoro system ten ma być wykorzystywany do okresowego sprawdzania bezpieczeństwa, to kluczowe jest, żeby baza ta była możliwie kompletna.

Warto zwrócić uwagę na dwa czynniki:

- Jakie testy może wykonywać skaner? Pełna lista powinna być dostępna na stronach www producenta.
- Jaki jest czas reakcji producenta na ujawnienie nowego zagrożenia? Inaczej mówiąc – ile czasu minie od publicznego ujawnienia informacji o nowym błędzie w Oracle, do opracowania przez producenta skanera odpowiednich reguł skanowania i dostarczenia ich do użytkownika.

Sposób uaktualniania

Cechą która wiąże się z poprzednim punktem, jest sposób dostarczania przez producenta nowych uaktualnień. Najlepiej żeby był możliwie zautomatyzowany. Zwykle skaner ma możliwość sprawdzenia uaktualnień przez Internet przed rozpoczęciem każdego skanu.

Fałszywe alarmy

Ponieważ jak na razie skanery automatyczne nie dysponują inteligencją, zdarza się im popełniać błędy. Zwykle polegają one na podniesieniu fałszywego alarmu. Duża ilość takich alarmów niepotrzebnie obciąża administratorów, oraz sprzyja przeoczeniu prawdziwych problemów.

Jest to cecha bardzo zależna od konfiguracji i specyfiki testowanego środowiska. Jedynym sposobem jest przetestowanie skanera w naszej instalacji. Na szczęście większość producentów udostępnia wersje ewaluacyjne ograniczone czasowo.

Raporty

Bardzo ważną cechą jest sporządzanie raportów, prezentujących w sposób przejrzysty rezultaty działania skanera. Cóż nam po doskonałym skanerze, jeśli rezultatem jego pracy będzie lista zajmująca 100 stron?

Ważne jest też żeby skaner był w stanie sporządzać raport szczegółowy zawierający wskazówki jak usuwać znalezione błędy. Powinien to być raport czytelny zarówno dla administratora bezpieczeństwa, jak i dla administratora Oracle

Przykładowe skanery bezpieczeństwa dla Oracle

ISS - Database Scanner

http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_database.php

- Database Scanner jest produktem firmy Internet Security Systems. Skaner ten nie jest dedykowany tylko i wyłącznie do testowania instalacji Oracle. Jest to skaner produktów bazodanowych. Oprócz Oracle, potrafi on też sprawdzać MS SQL i Sybase. Tak więc jego wartość wzrasta dla instalacji heterogenicznych.
- Posiada bardzo bogaty zestaw funkcji, zwłaszcza w module audytowym. Może posłużyć zarówno do testowania Oracle jak i do dokumentowania instalacji i nadzorowania zmian.
- Baza zagrożeń jest aktualizowana dość często.
- Ma możliwość integracji z innymi narzędziami ISS – Internet Scanner, System Scanner.

- Żeby używać Database Scannera do sprawdzania Oracle, na komputerze na którym jest zainstalowany skaner, należy zainstalować również oprogramowanie klienckie dostępne na CD instalacyjnym Oracle. Skaner wymaga zainstalowania SQL*Net/Net8. W przeciwnym wypadku nie będzie umiał skomunikować się z Oracle.
- Jest to narzędzie „z górnej półki” i za to trzeba słono zapłacić

AppSecInc. - AppDetective for Oracle

<http://www.appsecinc.com/products/appdetective/oracle/>

- Firma Application Security Inc. dostarcza narzędzi testujących pod nazwą AppDetective. Na stronach producenta można zauważyć że jest to cała rodzina produktów (AppDetective for Oracle, MSSQL, Sybase, Lotus Domino, MS Exchange). Jednak zawsze jest to ten sam skaner, a jego funkcjonalność jest limitowana przez posiadaną licencję.
- Firma Application Security była pionierem jeśli chodzi o dostarczanie narzędzi testujących bezpieczeństwo dla Oracle. Inżynierowie tej firmy odkryli sporo nowych zagrożeń. Dzięki dobremu zapleczu technicznemu, które poszukuje nowych błędów, baza zagrożeń AppDetective jest bardzo aktualna.
- Skaner ten skupia się przede wszystkim na testowaniu bezpieczeństwa. Są obecne zarówno funkcje „testu penetracyjnego” jak i „audytu”. Funkcje inwentaryzacji są nieco uboższe.
- W tej chwili produkt nie jest dostępny w Polsce. Być może nasza firma wkrótce zajmie się jego sprzedażą.

NGSS – Typhon i OraScan

<http://www.nextgenss.com>

- Najwięcej doniesień o nowych zagrożeniach związanych z Oracle pochodzi ostatnio od Davida Litchfielda - założyciela firmy NextGeneration Security Software. Firma ta produkuje skaner bezpieczeństwa Typhon. W niedalekiej przyszłości pojawi się też skaner specjalizowany do systemów Oracle – OraScan. Na razie dostępna jest wersja beta. Jednak w skanerze uniwersalnym – Typhon są obecne wszystkie nowe testy dotyczące Oracle.
- Skaner ten skupia się przede wszystkim na bardzo dokładnym testowaniu frontendów do danych, a więc przede wszystkim serwera www Apache wraz z modułami napisanymi przez Oracle służącymi do udostępniania aplikacji PL/SQL, JSP, SQLJSP, XSQL.
- Będzie to prawdopodobnie produkt dedykowany dla Oracle Application Server.
- Na razie jest to jeszcze produkt niedojrzały. Nie oferuje np. zaawansowanych funkcji raportowania.
- Może stanowić dobre uzupełnienie innych produktów.
- Warto mieć na niego oko w przyszłości, gdyż za tą firmą stoją wysokiej klasy specjaliści.
- Można go kupić przez Internet na stronie producenta.

Narzędzia OpenSource – Nessus

<http://www.nessus.org>

- Świetnym uzupełnieniem narzędzi komercyjnych może być skaner spod znaku Open Source – Nessus.
- Jest to ogólny skaner sieciowy, jednak posiada bardzo aktualną bazę zagrożeń. Również tych dotyczących Oracle.
- Nie jest w stanie wykonywać testów bezpieczeństwa polegających na zdalnej analizie konfiguracji („audytów”)

Podsumowanie

Narzędzia do testowania bezpieczeństwa Oracle uzupełniają wiedzę administratora Oracle o wiedzę z zakresu bezpieczeństwa. Dlatego też uważam że powinny znaleźć zastosowanie w każdej organizacji, która przechowuje swoje dane na systemach Oracle. Należy jednak pamiętać że nie jest to cudowny lek, który sprawi że nasze serwisy będą w 100% odporne. Pamiętajmy o tym że zwykle najsłabszym ogniwem w łańcuchu bezpieczeństwa jest człowiek, a więc błędy programistów aplikacji czy też błędy administratorów. Części tych błędów nie wychwyci nawet najlepszy skaner.