Wybrane metody ataków na systemy Oracle

Warsztat – PLOUG'2

Wojciech Dworakowski

Oracle

- Do niedawna uważany za system bezpieczny
- Powód: brak badań
  - brak dostępu do software
  - brak zainteresowania badaczy produktami komercyjnymi
- Od roku – znaczny wzrost zainteresowania
  - kilkanaście raportów na temat błędów
  - znajdowane błędy z reguły mają charakter dość poważny

Agenda

- Konta i hasła standardowe
- Pliki w bazy w systemie operacyjnym
- Oracle Listener
- Protokół SQL*Net
- Błędy w programach z ustawionym bitem SUID
- Serwer Apache z mechanizmem Servlet (Tomcat)
- Inne rodzaje (trywialnych) ataków
- Test penetracyjny Oracle 8.1.7/Linux
- Dalsze regiony poszukiwań.....

Środowisko testowe

- Linux (Debian)
- Oracle 8.1.7.0.0 Enterprise Edition
- Konfiguracja defaultowa
- Nie zainstalowane żadne patche

- Cel: Odnalezienie zagrożeń w instalacji standardowej

Konta i hasła standardowe

- Oracle instaluje wiele kont standardowych
- W internecie są dostępne listy kont i haseł standardowych
- Zawsze jest instalowanych kilka kont
  - Linux: 9
  - WindowsNT: 11
- Dwa konta – dobrze znane – system przy instalacji prosi o zmianę haseł:

SYS/CHANGE_ON_INSTALL	SUPERUSER,DBA
SYSTEM/MANAGER	DBA

Konta standardowe – nasze doświadczenia

- 17 użytkowników założonych przy instalacji

```
SQL> select username from dba_users
```

- Część to konta „demo”

```
SCOTT/TGER, ADAMS/WOOD,
  BLAKE/PAPER,....
```

- Większość to konta systemowe:

```
SYSTEM/MANAGER, CTXSYS/CTXSYS,
  MDSYS/MDSYS, TRACESVR/TRACE,....
```

Konta standardowe

Trzy konta standardowe mają bardzo wysokie przywileje:

TRACESVR/TRACE, MDSYS/MDSYS, CTXSYS/CTXSYS

```
SQL> select * from dba_role_privs
     2  where granted_role='DBA';     <---  SYS, SYSTEM i
CTXSYS (!)

SQL> select * from dba_sys_privs
     2  where grantee='TRACESVR';     <---- create session,

select any  table

SQL> select * from dba_sys_privs
      2  where grantee='MDSYS';        <--- Bardzo wysokie
```

Scenariusz ataku

- Zalogować się jako nieuprzywilejowany user
- select username from all_users
- Sprawdzić czy są użytkownicy standardowi (porównać z listą kont sandardowych)
- Spróbować zalogować się

Konta standardowe

- Nie wszystkie znane konta standardowe są zawsze instalowane
- Część jest w bazach demo lub przy instalacji opcji dodatkowych
- Przeszukanie wszystkich plików w instalacji Oracle wykazuje:
  - Linux: 52 konta, w tym 11 z wysokimi przywilejami
  - Windows: 57 kont, w tym 11 z wysokimi uprawnieniami

Konta standardowe – pytania

- Nie wiemy które z kont systemowych można usunąć?
- Jaka funkcjonalność Oracle nie będzie przez to dostępna?
- Czy dla wszystkich kont systemowych można zmieniać hasło?

Pliki Oracle w systemie operacyjnym

- Większość jest instalowana w $ORACE_HOME
- Plik /etc/oratab
  - do odczytu dla wszystkich
  - można uzyskać informacje o:
    SID, ORACLE_HOME

Pliki w $ORACLE_HOME

- Większość plików może być czytana przez wszystkich
- Czy również pliki z danymi?
- Istnieją narzędzia do wyłuskiwania informacji z pliku bazy

Pliki w $ORACLE_HOME

- Pięć plików ma prawdopodobnie źle ustawione atrybuty

```
root@oracle# find . -type f -and -perm -o+w -exec ls -l {} \;
-rwxr-xrwx    1 oracle   oinstall ./Apache/Jserv/logs/jserv.log
-rwxr-xrwx    1 oracle   oinstall ./Apache/modplsql/bin/modplsq
-rw-r--rw-    1 oracle   oinstall   ./otrace/admin/collect.dat
-rw-r--rw-    1 oracle   oinstall  ./otrace/admin/facility.dat
-rw-r--rw-    1 oracle   oinstall  ./otrace/admin/regid.dat
```

Pliki SUID/SGID

- 4 pliki – 1 SUID root (niedostępny publicznie), 2 SUID oracle (dostępne), 1 błędnie skonfigurowany

```
root@oracle# find . -type f -and -perm +6000 -exec ls
l {} \;
    -rwsr-s---    1 root       oinstall ./bin/dbsnmp
    -rwsr-s--x   1 oracle   oinstall ./bin/oracle
    -rwsr-s--x   1 oracle   oinstall ./bin/oracle0
    -rwSr-----     1 oracle   oinstall ./dbs/orapwora1
```

Pliki SUID/SGID

- W programie dbsnmp jest błąd pozwalający na uruchomienie dowolnego kodu z przywilejami programu (root !)
- Czym może grozić zdjęcie uprawnień SUID/SGID z tych plików ???
  - oracle, oracle0 – znaczna degradacja wydajności (wg. informacji z list dyskusyjnych)
  - dbsnmp - ???

Oracle Listener

- Proces do komunikacji klientów sieciowych z bazą Oracle
- Standardowo nasłuchuje na porcie 1521/tcp
- Komunikacja:
  - Protokół SQL*Net
  - W niższej warstwie – protokół TNS
- „Pięta achillesowa” systemu Oracle !

Błędy w tnslsnr

- Bez żadnej autoryzacji, komunikując się z portem listenera można zdalnie uzuskać bardzo dużo informacji o systemie:
  - wesja oprogramowania Oracle
  - wersja i rodzaj systemu operacyjnego
  - czas od uruchomienia
  - ścieżki do logów
  - opcje listenera (m.in. security)

Błędy tnslsnr (c.d.)

- rodzaj serwisów Oracle obsługiwanych przez listener
- argumenty wywołania
- kompletne środowisko (wszystkie zmienne) !!!
- ...

- Standardowo dostęp nie jest zabezpieczony hasłem
  - możliwe zdlane zastopowanie serwisu – bez żadnej autoryzacji !

Nadpisanie dowolnego pliku

- Manipulacja parametrami protokołu TNS umożliwia zmianę pliku, do którego wędrują logi Listenera
- W rezultacie można utworzyć lub nadpisać dowolny plik, do którego ma dostęp użytkownik *oracle* !
- Listener loguje informacje o błędach w zapytaniach, cytując w logu całe błędne zapytanie

Scenariusz ataku

- Zdalnie – wysyłając odpowiednie zlecenie TNS, przestawiamy plik logu Listenera na: /home/oracle/.rhosts
- Łączymy się ponownie i wysyłamy błędne zlecenie TNS, w którego ciele jest string: wojdwo 10.1.1.223
- W rezultacie w .rhosts użytkownika oracle jest wpis: wojdwo 10.1.1.223
- Możemy zdalnie zalogować się na serwer, na konto usera oracle, bez żadnej autoryzacji !

Skutki ataku

- Uprawnienia początkowe:
  - Żadne – zdalny user z możliwością wysyłania pakietów do listenera (1521/tcp)
- Uprawnienia po ataku:
  - Użytkownik oracle na serwerze
  - Pełny dostęp do danych

Ujawnienie informacji o poprzedniej sesji

- Listener nie czyści bufora wejściowego
- Można odczytać cały bufor, podając w nagłówku TNS, większą niż rzeczywista długość pakietu
- W rezultacie można odczytać część poprzedniego zlecenia TNS
- Może to być np. hasło DBA

Narzędzia

- Inny system unixowy
- Program do konstruowania pakietów TNS
  - tnscmd

Protokół SQL*Net

- Transmisja otwartym tekstem
- Podatny na podsłuch, przejmowanie i fałszowanie sesji
- Autoryzacja otwartym tekstem, lub przez przesłanie zaszyfrowanego hasła
  - możliwość podsłuchania hash-a i prób brute-force

Błędy w programach wchodzących w skład Oracle

- dbsnmp – SUID root
- Prawdopodobnie umożliwia wykonanie dowolnego kodu, z uprawnieniami root-a
- Możliwe przepełnienie stosu w zmiennej $ORACLE_HOME

```
wojtekd@oracle:~$ export ORACLE_HOME=
`perl -e 'print "A"x1000'`
wojtekd@oracle:~$
wojtekd@oracle:~$ dbsnmp
    Segmentation fault
```

Błędy w innych programach

- Debugowanie procesu dbsnmp wskazuje na możliwość skutecznego wykonania ataku
- Potwierdzają to inne źródła
- Źródła internetowe mówią także o podobnym błędzie w innych programach z ustwaionym bitem SUID (dot. <8.1.5)

Apache/Tomcat

- Serwer WWW z mechanizmem Servlet
- Apache 1.3.12 Jserv/1.1 mod_perl/1.22
- W oprogramowaniu tym nie są znane żadne poważne błędy
- Małe zagrożenie:
  - Wysłanie zapytania o nieistniejący plik .jsp, ujawnia ścieżkę dostępu do serwisu www i plików .jsp
  - Zbędny skrypt /cgi-bin/test-cgi , ujawniający szczegóły konfiguracyjne

Apache/Tomcat

- Apache działa z takimi uprawnieniami, jak użytkownik, który go uruchamia
- Serwer WWW należy uruchamiać z innymi uprawnieniami niż bazę danych
- Standrdowo Apache jest uruchamiany z takimi samymi prawami (użytkownik oracle)

Trywialne ataki

- Przeglądanie skryptów SQL w poszukiwaniu haseł zapisanych na stałe
- Przeglądanie listy procesów w poszukiwaniu haseł podanych jako argument wywołania programu

```
wojtekd@oracle:~$ ps auxw | grep svrmgrl
kravietz  pts/2    S    23:30   0:00 svrmgrl
system/manager
```

Trywialne ataki

- Zdobycie plików backupu bazy
  - Odtworzenie bazy na innym serwerze
- Podsłuchanie transmisji sieciowej
- Atak na system operacyjny
  - Pozyskanie plików z danymi