ADITYA K SOOD, A.K.A.
0KN0CK

Auditing Oracle in a Production Environment

Difficulty

This paper is based on real penetration testing of Oracle servers on HP-UX systems and the way the auditor has to follow to combat the stringencies that come in a way. We will dissect the errors and the way to bypass them to conduct the tests.

Usually Oracle is used as a backend in large production environments supporting applications like SAP and other products. The production environment is very critical from company perspective and data is one of the prime concerns that has to be protected. That's why most of the attackers try to hack the databases to leverage maximum information. We will specifically cover the penetration testing of Oracle servers. The prime target is to test the Oracle by using core techniques in a tactical way. We will talk about core Oracle processes running in a network and the way to audit it. The essential point is to bypass the generic problems thereby conducting a pure audit of an Oracle database.

Understanding Oracle Services from Hacker's Perspective

The Oracle database is used in a distributed way to support a number of data centric applications. Being client server architecture the main database is supported on the prime server and all the other nodes communicate with it by connecting to the Oracle server. For Example: in SAP organization (i.e. System Application Programming) software supports Oracle at the backend. All the clients have a direct interface to the application running on server with an Oracle database on the backend. It is good to dig little more to understand the Oracle processes running in the network. To understand the Oracle functioning from pen testing point of view, the underlined components need to be traversed. So let's start with it.

Oracle XML DB Service

While scanning the network, the auditor will always find the Oracle XML DB Service. Basically it is implemented for the HTTP based working environment where web applications are supported. The second reason for the use of XML db is to store data in XML format for productive use in cross platforms. As XML is a strategic part of DOM (i.e. Document Object Model) so data can move in and out through DOM interface. The mechanisms like content generation and transformation with superior memory management are supported effectively by Oracle. From a network perspective protocols like HTTP, Web DAV and FTP are well supported. It also favors the SQL repository search through XML. The SQL dual operations (i.e. SQL operation) can be carried on XML and XML operations can be carried on SQL. This web service basically runs on port 80 or port 8080. This service can be a good response revealer when a HTTP Verb request is sent to the server. The auditor always sends a GET /POST/HEAD request to the desired port for querying Oracle VERSION Check. It answers back with good information and the Oracle version running. It's a good technique to follow. Let's have a look at the network map output (see Listing 1).

This gives a view that the service port is open and it can process the service request.

WHAT YOU WILL LEARN...

The user will learn about the methodology and how to conduct tests.

The user will learn about Oracle Auditing Model.

The way to penetrate deep into systems.

Overall Oracle deployment and responsible behavior of disclosing bugs.

WHAT YOU SHOULD KNOW...

Understanding of Oracle working and implementation.The administration knowledge of Oracle suit will be added advantage.

Deployment of Oracle in a production environment.

Knowledge of basic Oracle tools.

Oracle MTS Service:

Oracle provides support to Microsoft Transaction Server for carrying out operations where COM components are involved. As Oracle works in distributed structure model where number of clients connect to main server, this service proves beneficial. This service is implemented through OCI (i.e. Oracle Call Interface). The process listed for this service is OMTSRECO.exe which runs in the context of running Host. The MTS acts as a distributed transaction coordinator to manage and control the transactions taking place in a distributed way. The transactions are controlled by placing a proxy component termed as Oracle MTS (i.e. OraMTS) between database and DTC. Firstly all the working behavior is based on communication between the processes but with new features the paradigm has shifted to intra processes. This provides per process control over the transaction taking place. The MSDTC supports the OraMTS. It is straight forward depicts that Host running the Oracle MTS service will be a Windows machine. Let's look at the scanned output (see Listing 2).

The scanned output shows port 2030 when allowing the Oracle MTS service. With this service MSDTC is implemented. On patched versions of Microsoft Windows the MSDTC is a serious vulnerable base for exploiting the system.

Oracle TNS Listener Service

The Oracle TNS Listener Service is a centralized point where every single node of a system connects. Basically *the TNS* listener is supported well in database clusters and even centralized servers in a production environment. The client connects to the server through the listener to run queries directly on the database with connect calls. All the queries are executed remotely and the changes take place in the Oracle database. The TNS means Transport Layer Substrate. It manages the remote command execution mechanism and traffic between client and server. The Oracle suite is comprised of the TNS listener component for server side and the TNS Control component on client side. The connection is initiated through TNS control utility which is accepted by the TNS Listener. The TNSNAMES.ORA and SQLNET.ORA are the configuration files for the TNS listener. But for effective use the auditor has to create a LISTENER.ORA with same configuration semantics as described in the other two files. The prime aim is to set a connection string coupled with the type of service requested from the Oracle server. When the SQL*PLUS is executed for interactive query execution, it checks the service type. If the service type is not specified and not supported by the Oracle server, the TNS listener fails to set the connection (see Listing 3).

That's the exact way to set the listener. The service name is critical to set a client properly. It generates many errors with a badly configured parameter. This point comes into play when the auditor has to set a client while testing. This strategy will be discussed with thin clients in the next part. So let's have a look at the scanned output (see Listing 4).

The Oracle TNS Listener is a high risk vulnerability issue when not applied properly. The output shows that the default port 1521 which is in listening state. By conducting further fingerprinting one can analyze whether this component is vulnerable or not.

These three processes constitute the Oracle working in a high end production environment. This needs to be understood efficiently when an audit is to be conducted.

What Leads to Oracle Hacking?

The Problems that lead to hacking of Oracle Servers in Production Environment:

- It has been identified that cost optimization leads to insecurity of products. It seems to be a bit odd but this is the truth. The organization finds it difficult to move from older version of softwares to newer one because of incurring costs. This seems a bit sarcastic because no money is spent on security and privacy of running components. So some older versions of software run in organizations for longer durations without considering the risk.
- Even the older versions of software are not regularly tested or patched against certain vulnerabilities. The patch management process is not followed by the company which opens doors for hackers to compromise the security.
- To illustrate the above issues it has been revealed that organizations run old versions of Oracle without

Listing 1. *Oracle XML DB Service*

```
5302/tcp open  X11          HP MC/ServiceGuard
5303/tcp open  hacl-probe?
6000/tcp open  X11?
6112/tcp open  dtspc?
8080/tcp open  http       Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i
                      Enterprise Edition Release)
```

Listing 2. *Oracle MSDTC Service*

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 2000 microsoft-ds
2030/tcp  open  oracle-mts   Oracle MTS Recovery Service
2301/tcp  open  http         HP Proliant System Management 2.0.1.104
                      (CompaqHTTPServer 9.9)
3372/tcp  open  msdtc        Microsoft Distributed Transaction Coordinator (error)
```

Listing 3. *TNS Connection String*

```
KNOCK =
  (DESCRIPTION = (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = somehost)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME=ORA10)
    )
  )
```

moving to newer ones. Oracle 9 is still supported without migration to Oracle 10 or Oracle 11. Even no patches are applied. This type of software and path management put organizations at risk.

- The poor configuration and default settings of components and software are one of the prime factors of insecurity. There is no doubt administering Oracle is not an easy task. One has to be aware of each and every aspect of software from a security point of view prior implementing in the organization. But looking at the scale on which Oracle servers are implemented, this has to be verified to protect the insecurity. Default passwords and schemas are a hacker's first choice.
- Information obtained through Banner Grabbing is one of the best sources to check the version and state of software running. The administrators have to remove it or display it in a rogue way that becomes hard to decipher. This is a good approach of protecting information.

These are some of the manipulative components that allow the attackers to break into databases.

A Way the Hacker Performs Audit

Now we will discuss things to look into while performing an Oracle audit. It's always better to start the process from top to bottom to query entities one by one. It is a good approach to obtain as much knowledge of the target by performing a number of different requests and using many different tools. We will follow the Oracle Auditing Model specifically outlined in this paper. Let's analyze the process in steps:

Understanding the Deployed Oracle Environment

Auditing an Oracle server requires an in depth understanding of the environment in which it is deployed. It's very critical from organization's point of view if any of the Oracle servers go down while auditing. Auditing should not result in downtime of production servers. It is unacceptable on auditors behaf because it results in business loss. For this reason certain steps must be followed by an auditor to perform secure auditing. For Example: exploit testing should be carried out after normal working hours. While performing an audit all steps to protect organization should be taken.

The underlined diagram is the standard Oracle approach. Thanks to Oracle for this (see Figure 1).

After this, Oracle testing is conducted. For simplification of concept we will use the Oracle Auditing Kit for this.

Oracle Servers Alignment

It is one of the starting step in which an auditor checks how the Oracle servers are set for working. Whether clusters are designed every node is in virtual state with virtual server. The other setting can be direct connection interface to the server. Both connections work on the concept of OCI (i.e. Oracle Call Interface). This information needs to be collected. It can be done by looking at the network architecture or by consulting with the security team in a general manner. One should gather the stats whether the target is dedicated or virtual in nature. A generalized view is presented at Figure 2.

Oracle Service Scanning

The next step is to perform the simple scanning for the default ports for the Oracle services. This provides an overall insight of the open ports and the type of services running on the network. Mostly in organizations and large scale environments the standard ports are used. So scanning should be done in a silent way without generating much traffic. Of course NMAP is the best tool to use for our scanning purposes. Let's see Listing 5

I have truncated the output for better view. All three processes are in listening state. You can follow by performing a simple step to check whether the TNS listener is in listening state or not. The Oracle client setup has a utility called TNSPING which automatically detects the state whether it is alive or not. So it's a good step to perform.

Oracle Version Detection

The Oracle version is required for understanding the type of vulnerabilities it possesses. The Oracle version provides the key information to set a diversified attack surface and testing entities. The version should be known prior carrying out

Listing 4. *Oracle TNS Listener Service*

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
1067/tcp open  msrpc         Microsoft Windows RPC
1521/tcp open  oracle-tns    Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)
2030/tcp open  oracle-mts    Oracle MTS Recovery Service
3389/tcp open  microsoft-rdp Microsoft Terminal Service8080/tcp open  http
Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i Enterprise Edition Release)
```

Listing 5. *Scanning for Oracle Service through Nmap*

```
[root@knock] nmap -P0 -sV -O -v -T aggressive 172.16.25.5 -p 1521, 8080 , 2030
Host 172.16.25.5 appears to be up ... good.
Interesting ports on 172.16.25.5:
Not shown: 1681 closed ports
2030/tcp  open  oracle-mts    Oracle MTS Recovery Service
8080/tcp open  http       Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i
                       Enterprise Edition Release)
1521/tcp open  oracle-tns    Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)
```

Listing 6. *Oracle Version Check via HTTP XML DB*

```
HTTP/1.1 501 Not Implemented
MS-Author-Via: DAV
DAV: 1,2,<http://www.oracle.com/xdb/webdav/props>
Server: Oracle XML DB/Oracle9i Enterprise Edition Release 9.2.0.1.0 - 64bit Production
Date: Wed, 30 Jul 2008 05:58:22 GMT
Content-Type: text/html , Content-Length: 208
```