EC-Council Licensed Penetration Tester

Methodology: Database Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Test 1: Identify the password management in Oracle

Target Organization	
URL	
Oracle Accounts Using Weak Passwords	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Retrieve the information about the database via a vulnerable web application

Target Organization	
URL	
Retrieved Database Information via Error Messages in Vulnerable Web Applications	1. 2. 3. 4. 5.
Syntax Used in the Login Box to Retrieve Information about the Database	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Identify execution of public privileges on Oracle

Target Organization	
URL	
Identified Execution of Public Privileges on Oracle	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Identify privilege escalation via cursor technique in Oracle

Target Organization	
URL	
Identified Privilege Escalation Using Cursor Technique in Oracle Database	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Identify public privileges from object types

Target Organization	
URL	
Identified Public Privileges from Object Types	1. 2. 3.
Transferred Data Out of the Database Using SQL Injection Attacks	1. 2. 3. 4.
Oracle Audited Entries	1. 2. 3. 4. 5.
SQL Statement Submitted by the Database	1. 2. 3. 4. 5.
Information Gathered from Audited Tables	1. 2. 3. 4. 5.

Attacks that can Bypass the Protections Provided by the Oracle Database Vault	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Identify Oracle Java vulnerabilities in SQL injection

Target Organization	
URL	
Identified Oracle Java Vulnerabilities in SQL Injection	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Determine Oracle service ID (SID) using Metasploit

Target Organization	
URL	
Techniques Used to Determine the Service ID	1. 2. 3.
Determined Oracle Service ID (SID) Using Metasploit	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Determine Oracle version using Metasploit

Target Organization	
URL	
Determined Oracle Version Using Metasploit	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Identify attack into database target DB by using a simulated user

Target Organization	
URL	
Script to Detect Flaws of the DBMS_METADATA.GET_DDL Function in Oracle	
Identified Attack into Database Target DB by Using a Simulated User	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 10: Scan for default ports used by the database

Target Organization		
URL		
Default Ports Used by the Database	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.	21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40.
List of Open Ports Discovered on a Computer/Server	1. 2. 3. 4. 5.	

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Scan for non-default ports used by the database

Target Organization		
URL		
List of Non-Default Ports Used by the Oracle Database	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.	11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 12: Identify the instance names used by the database

Target Organization	
URL	
Unique Names Specified While Configuring an Instance of the Notification Services	1. 2. 3.
Identified Instance Database Objects	1. 2. 3. 4.
Instance Name Criteria	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Identify the version numbers used by the database

Target Organization	
URL	
Identified Version Numbers Used by the Database	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Attempt to brute-force password hashes from the database

Target Organization	
URL	
Passwords Identified from the Database Using Brute-Force Password Hashes	
Location of Oracle Password Hashes	1. 2. 3. 4.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 15: Sniff database-related traffic on the local wire

Target Organization	
URL	
Number of Database Connections Determined with Sniffing Technique	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16: Microsoft SQL Server testing

Target Organization	
URL	
Various Microsoft SQL Server Testing Techniques	1. 2. 3. 4. 5. 6.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.1: Test for direct access interrogation

Target Organization	
URL	
Directly Accessed Data Structures	
Special Queries Used to Directly Interrogate the Database	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.2: Scan for Microsoft SQL Server ports (TCP/UDP 1433)

Target Organization	
URL	
Services Delivered over the Incoming TCP Connections through Port 1433	1. 2. 3.
Scan Results for Microsoft SQL Server Ports	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.3: Test for SQL Server Resolution Service (SSRS)

Target Organization	
URL	
Referral Services Provided For Multiple Server Instances Running on the Same Machine	
UDP port 1434 Scan Results for SQL Server Resolution Service	
Hidden Database Instances	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.4: Test for buffer overflow in the pwdencrypt() function

Target Organization	
URL	
Unchecked Buffer in the Password Encryption Procedure	
Identified Incorrect Permission on the SQL Server Service Account Registry Key	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.5: Test for heap/stack buffer overflow in SSRS

Target Organization	
URL	
Scan Results for the UDP port 1434 at the firewall	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.6: Test for buffer overflows in the extended stored procedures

Target Organization	
URL	
List the Extended Stored Procedures that Cause Stack Buffer Overflow	
Publicly Accessible Database Queries	
Loaded and Executed Database Query that Calls One of the Affected Functions	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.7: Test for service account registry key

Target Organization	
URL	
Test Results for the Altered SQL Service Account Registry Key	1. 2. 3. 4. 5.
Escalated Privileges that Weaken the Security Policy of SQL Server	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.8: Test the stored procedure to run web tasks

Target Organization	
URL	
Test Results for the Stored Procedure to Run Web Tasks	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.9: Exploit SQL injection attack

Target Organization	
URL	
Details of the Database	1. 2. 3. 4. 5.
Special Queries Run to Gain Access to the Database	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.10: Blind SQL injection

Target Organization	
URL	
Exploited Web Applications and Back-End SQL Servers	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.11: Google hacks

Target Organization	
URL	
SQL Server Errors Searched by Google	1. 2. 3. 4. 5.
List the Google Queries at Johnny Long's "Google Hacking Database"	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.12: Attempt direct-exploit attacks

Target Organization	
URL	
Code Injection Performed to Gain Unauthorized Command Line Access	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.13: Try to retrieve the server account list

Target Organization		
URL		
Server Account List		
SQL Login IDs		Data of the Connected Servers
1.		1.
2.		2.
3.		3.
4.		4.
5.		5.
Commands Used to Access the Account List		
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 16.14: Using OSQL, test for default/common passwords

Target Organization	
URL	
Test results for Default/Common Passwords Using OSQL	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.15: Try to retrieve the sysxlogins table

Target Organization	
URL	
Information Collected for SQL Server	

Stored Information in Sysxlogins System Table	
Qualified User Names	Group Names
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 16.16: Brute-force the SA account

Target Organization	
URL	
Retrieved Password by Brute-forcing SA Account	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17: Port scan UDP/TCP ports (TCP/UDP 1433)

Target Organization	
URL	
Techniques Used for Port Scan	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17.1: Check the status of the TNS Listener running at Oracle server

Target Organization	
URL	
Status of the TNS Listener Running at Oracle Server	
SID Retrieved for Unprotected Listener	
Files that Control the Listener	1. 2. 3. 4. 5.

Mode Used to Configure a Listener		
☐ Database	☐ PLSExtProc	☐ Executable

Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17.2: Try to log in using default account passwords

Target Organization		
URL		
Attempted Log in Using Default Account Passwords		
Account	Password	
1.	1.	
2.	2.	
3.	3.	
4.	4.	
5.	5.	
6.	6.	
Attempted Login Successful	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 17.3: Try to enumerate SIDs

Target Organization	
URL	
Default User Names and Passwords after SID Enumeration	
User Names	Passwords
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 17.4: Use SQL *Plus to enumerate system tables

Target Organization	
URL	
Command Used to Establish a Connection to a Remote User	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18: MySQL server database testing

Target Organization	
URL	
Techniques Used for MySQL Server Database Testing	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18.1: Port scan UDP/TCP ports (TCP/UDP)

Target Organization	
URL	
Scan Results for TCP/UDP Ports for MySQL Server Database Services	1. 2. 3.
Information Gathered from Scan Results	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18.2: Extract the version of the database being used

Target Organization	
URL	
Extracted Version of the Database Being Used	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18.3: Try to log in using default/common passwords

Target Organization	
URL	
Attempted Login Using Default/ Common Passwords	
User Names	Passwords
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18.4: Brute-force accounts using dictionary attack

Target Organization	
URL	
Brute-forced Accounts Using Dictionary Attack	
Methods Used to Brute-Force Accounts	
☐ Manually	☐ Making Use of Software and Database
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 18.5: Extract system and user tables from the database

Target Organization	
URL	
Extracted System and User Table Information from the Database	
System Information	User Table Information
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

