iGNITE
Technologies

# MSSQL

## SECURITY ASSESSMENT

### ADVANCED PENTEST TRAINING


www.ignitetechnologies.in

# MSSQL S.A.

This Security Assessment will examine for SQL Server instance discovery, inadequate configuration auditing, and privilege escalation at scale. Penetration testers and red teams are the primary targets of this operation. However, manual assessment supports a number of methods that administrators may utilise to inventory the SQL Servers in their ADS domain.

Additionally, a company can use this approach to define the risk factor and ensure compliance with information security policies. They can also use it to assess their level of reaction to any cyber-based threats. APTs primarily use Privilege Escalation after gaining a foothold to complete their objectives by using administrative or root accounts.

## PREREQUISITES

Should be aware of basic computing, operating system, file types, hashing & encoding and networking fundamentals.

**COURSE DURATION: 20 to 25 HOURS**

## LAB SETUP

- SQL Configuration
- Configure Vulnerable SQL Instances
- Link Database
- Create Trusted Database
- Pentest Lab setup

## Enumeration

- Users / Roles
- Databases
- Tables
- Sensitive Data

## Privilege Escalation

- Impersonation
- Trustworthy Database

## Database Link Abuse

- Enumerating Database Links
- Executing Commands

## Gaining Access

- Metasploit
- Nmap
- Nessus
- Sqlping
- Powersupsql
- sqlcmd/osql
- Brute Forcing

## Command Execution

- Xp_cmdshell
- Extended Stored Procedures
- CLR Assemblies
- OLE Automation Procedures
- External Scripts

## Persistence

- Startup Stored procedures
- Dumping Hashes