利用 Nmap 对 MS-SQLSERVER 进行渗透

如今 Nmap 的脚本引擎从一个普通的端口扫描器转变为具有攻击性的渗透测试工具 。随着 nmap 各种脚本的存在。到目前为止，我们甚至可以进行完整的 SQL 数据库渗透而不需要任何其他的工具。

在本教程中，我们将看到在这些脚本中有些什么样的信息，以及如何通过 Nmap 从数据库中提取，还可以利用 SQLServer 来执行系统命令。

默认 MS-SQL 数据库上运行的端口为 1433，为了及时发现有关数据库，我们需要执行以下脚本：

已经获取了数据库的版本和实例的信息。下一步检查是否有弱口令和数据库身份验证，需要运行以下 nmap 的脚本，它会执行暴力破解。

（nmap 暴力破解 MS-SQL 账户）

可以看到，没有发现任何数据。在这种情况下可以利用这个脚本来使用我们自己的用户名和密码字典，以便及时发现有效的数据库帐户。使用这个命令：

```
nmap -p1433 – script ms-sql-brute – script-args userdb=/var/usernames.txt,passdb=/var/passwords.txt
```

还可以尝试另一种脚本，来检查 Microsoft SQLServers 是否存在空密码。

现在我们知道 sa 帐户没有密码。我们可以使用这个信息来连接数据库直接执行脚本,需要进一步 Nmap 有效身份认证。如果我们想知道在哪个数据库 sa 帐户访问或任何其他账户,可以运行 ms-sql-hasdbaccess 脚本与下列参数:

（查看某用户访问了哪些 DB）

通过 Nmap 查询 Microsoft SQL Server 来获取数据库表。

SQL Server 2000 的 xp_cmdshell 默认情况下是启用的,因此我们甚至可以执行操作系统命令。通过 Nmap 脚本中可以看到下面的图片：

（通过 xp_cmdshell 来运行 OS 命令）

（通过 xp_cmdshell 来运行’ net users’ ）

最后还可以运行一个脚本来提取数据库，利用哈希值破解密码。工具：john the ripper

因为只有一个空口令的 sa 数据库帐户，所以没有任何的哈希值。