Executive Summary

Ryan Boyce

February 20, 2017

MySQL Exploit with Metasploit

**INTRODUCTION**:

This report summarizes the vulnerabilities that exist in the Metasploitable Operating System, how to exploit the MySQL Server instance running on this OS, and how data can be extracted/corrupted with Metasploit and Kali Linux. The exploits detailed in this summary were conducted on February 19, 2017. While Metasploitable is an overly vulnerable version of Linux, it is an excellent way of showing how real exploits would take place on regular versions of Linux such as Red Hat, Ubuntu, or SUSE.

The scan conducted against the Metasploitable virtual machine revealed several critical flaws in the Metasploitable Linux operating system. It was found that an FTP service was running with anonymous logins, an rpcbind service was running which maps to network shares on the server, and an Apache Tomcat/Coyote JSP engine was running. Towards the end of the scan, it was found that a MySQL Server instance was also running on the machine. Any one of these services can be exploited yet it was determined that targeting the MySQL server instance would be most effective as there was a potential to find highly sensitive, lucrative data within the tables. MySQL is an open-source relational database management system (<https://en.wikipedia.org/wiki/MySQL>). This application allows for remote connection from a command prompt if the machine IP, username, and password are provided. If a username for the database can be determined and security flaws exist (weak password/no password requirements), access can be gained to the database without having SSH or RDP connections to the machine itself.

**OBJECTIVE**:

The objective of the scan and exploit is to show that, with poor or no username/password requirements on a MySQL Server instance, gaining access to and extracting data from that system is possible. It is the purpose of this executive summary and the slides that accompany it to reveal how malicious hackers can gain entry to an exposed database server.

**CONCLUSION**:

To avoid the data exposure and corruption detailed in this report, it is suggested that strong passwords be enforced in any environment but especially within a database instance. It is also suggested that, unless absolutely necessary for production usage, remote access to MySQL Server be eliminated. Lastly, while it is out of the scope of this document, it should be noted that any services running on the machine that are not mandatory be removed.