Executive Summary

Ryan Boyce

October 27, 2016

Nessus Scanning

Introduction:

The following report details a Nessus Scan of a machine running Metasplotiable. Metasploitable is an intentionally vulnerable operating system built off the Linux kernel. Compared to other Linux based operating systems such as Red Hat or Fedora, Metasploitable leaves certain services or features less secure or disabled so, during a scan, a penetration tester will see what vulnerabilities look like. The purpose of any scan is to reveal where the weaknesses exist within systems. Often, it may be difficult to reproduce a potentially dangerous vulnerability on a live system and it is especially difficult to replicate what a vulnerability may look like on a production machine. It is in a company’s best interest, then, to use a system such as Metasploitable to reveal where the weakness lies and how it will be detected by malicious hackers. In the case of this report, the scan revealed flaws in the Metasploitable system that may exist elsewhere in the company’s environment. There were seven “critical” vulnerabilities in total. One of these, a weak service password, could easily allow a hacker to gain a shell into the system remotely.

Objective:

The objective of this report is to reveal what vulnerabilities potentially exist on Linux operating systems. The report will also provide ways in which to remediate the vulnerbailites.

Conclusion:

It has been determined to focus on the “critical” vulnerabilities that have been revealed by the scan. Open SSH/SSL, rexecd services, open ports, and a weak password for the VNC server are vulnerabilities that a hacker could potentially use to gain access to a Linux based system. In order to remedy these issues, it is concluded that any machine running Debian or Ubuntu be upgraded to the latest release, rexecd services be disabled immediately, any port that is open that is not mandatory by an application be closed, and, lastly, all passwords in the environment use an encryption technique such as OTP.