# Lab - Windows Privilege Escalation - Unquoted Service Path

# Overview

# In Windows, if the path to a service is not enclosed within quotes and is has spaces, the OS handles the space as a break and will treat the rest of the service path as an argument. The If the vulnerable service is running with SYSTEM privileges, the logged-on user will also gain those same SYSTEM privileges.

# If logged on user has write permissions with any of the folders in the service path, as an attacker they can drop a malicious executable in that folder to get a reverse shell as SYSTEM.

# Example

# Consider a vulnerable service whose start mode is auto-start, its executable path has spaces and is not wrapped in quotes and runs with the LocalSystem privilege level. If we have write access to a folder in that path, we can place an executable such as a reverse shell .exe payload in the folder that will execute when the service starts on system boot/reboot. Back on our attack machine, where we have a listener waiting, we should be presented with a Windows command prompt on our attacker’s machine running with SYSTEM privilege level.

# Lab Requirement

# Install of the latest version of VirtualBox with Extension Pack.

# One virtual install of Kali Linux updated and upgraded.

# One virtual install of Windows 10

# Begin the lab!