Windows Privilege Escalation – Unquoted Services

By HackHappy

Published: 2018-04-24 · Archived: 2026-04-05 18:13:45 UTC

So, you've popped a user shell on a windows box and now you're looking to escalate those privileges. Great! In this article we'll look at one method of elevating your privileges by exploiting unquoted system services.

A Windows service is a program that runs in the background similar to a *nix daemon. Often they are automatically started when Windows loads but they can also be started manually by a user or by other software. When installing a Windows service a registry key is created at *HKEY_LOCAL_MACHINESYSTEMCurrentControlSetservices* for the service along with several values. One of those values is the *ImagePath* value seen in this image and is used to specify the location of the service executable.

In this image you can see the file path is not surrounded by quotes and becomes a candidate for escalating our privileges. When a Windows service is started the *CreateProcess* function is used to start the service executable. If the *ImagePath* value is not surrounded by quotes the *CreateProcess* function must try to interpret the correct path to the service executable. For example, if the *ImagePath* value contained *c:program filessub dirprogram name* then the function would attempt to execute the following:

> **c:program.exe** filessub dirprogram name
> **c:program filessub.exe** dirprogram name
> **c:program filessub dirprogram.exe** name
> **c:program filessub dirprogram name.exe**

If any of these directories have weak permissions this allows us to place a malicious executable that Windows will run as SYSTEM allowing us to escalate our privileges. Now that we know how to take advantage of unquoted services let's look at how to find them. You could simply look through the registry checking each service but that would take some time. An easier method is to query WMI and retrieve all services and then filter the results. This can be accomplished by (Read more...)

Source: https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/