

getting a double quote by the xp_cmdshell

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-07/0096.html>

From: nobody (pentester@yahoo.com)

Date: 07/18/02

Date: Thu, 18 Jul 2002 10:29:22 -0700 (PDT)
From: nobody <pentester@yahoo.com>
To: pentest_list <pen-test@securityfocus.com>

Help,

I am aware of all that the xp_cmdshell can do once you have it and it runs with the authority/context that you need.

While dumpster diving for .bat, .sql, .log, .iss, .cmd or .bak files

I sometimes want to see the contents of the file with a quick NT DOS command:

```
xp_cmdshell "type c:\program files\esm\agent.iss"
```

The NT TYPE command works if I enclose the whole drive:\path with double quotes – the space in between the program files is the problem

I cannot figure out the syntax for adding double quotes around this – inside the above xp_cmdshell command.

I have searched the web and found good sql references – but have not found out how to get those "" inside the xp_cmdshell.

anyone ?

sending the file via TFTP is not always allowed or advisable – since most IDS can be easily setup to see all tftp get/puts – also – I am aware of the other ways to get the file – sharing out the drive etc..

Do You Yahoo!?

Yahoo! Autos – Get free new car price quotes

<http://autos.yahoo.com>

SecurityFocus Penetration: getting a double quote by the xp_cmdshell

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** Joe: "RE: SQL Injection Legalities"
- **Next in thread:** Ryan Russell: "Re: getting a double quote by the xp_cmdshell"
- **Reply:** Ryan Russell: "Re: getting a double quote by the xp_cmdshell"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]