

NULL sessions on Windows 2000 systems [Was: Re: [Full-disclosure] Re: It's not that simple...]

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0590.html>

From: Jean-Baptiste Marchand (jbm.lists_at_gmail.com)

Date: 08/18/05

Date: Thu, 18 Aug 2005 09:58:52 +0200

To: full-disclosure@lists.grok.org.uk

* yossarian <yossarian@planet.nl>:

- > *In the original X-Force paper named pipes were mentioned besides Null*
- > *Sessions. Does it need both or either one – the paper isn't clear on this?*
- > *The named pipes seem to have dropped from all discussion.... Anyway, never*
- > *broke anything by disabling them, either. This is a registry hack described*
- > *in the MS Hardening guides for 2000 and 2003 server. Just like Null*
- > *sessions. Elsewhere dunno, but probably, never bothered.*

A NULL session usually refers to an anonymous connection to the IPC\$ share, giving remote access to named pipes.

Some named pipes can be opened anonymously (these named pipes appear in the NullSessionPipes registry value), i.e. in the context of a NULL session.

In addition, 6 named pipes are hardcoded in Windows 2000 and can always be opened anonymously:

http://www.hsc.fr/ressources/presentations/null_sessions/img7.html

The recent PnP vulnerability (MS05-039) can be anonymously exploited on Windows 2000 systems with 139/tcp or 445/tcp open, *except* if the RestrictAnonymous registry value is set to 2.

This is because the only way to disable NULL sessions *entirely* on Windows 2000 is to set RestrictAnonymous to 2:

http://www.hsc.fr/ressources/presentations/null_sessions/img23.html

Please read my recent presentation about NULL sessions, many people seem to know about NULL sessions but fewer people really understand the technical details:

http://www.hsc.fr/ressources/presentations/null_sessions/

Full-Disclosure: NULL sessions on Windows 2000 systems [Was: Re: [Full-disclosure] Re: It's not that simple...]

--

Jean-Baptiste Marchand

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>