

# SMB – Windows Login/Logoff Mechanism

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-10/5458.html>

---

**From:** Dwayne P. Shrum ([dwayne@yougotus.com](mailto:dwayne@yougotus.com))

**Date:** 10/16/02

From: "Dwayne P. Shrum" <[dwayne@yougotus.com](mailto:dwayne@yougotus.com)>

Date: Wed, 16 Oct 2002 11:34:44 -0700

Just an idea...

what about WINS server showing who is logged in by the WINS messenger [03h] entries – since logging out releases them [status= Active, Released, or Tombstoned], you could sort by that service entry to see who is actively logged in to the domain. no?

Dwayne

>-----Original Message-----

>Hi,

>

>Can somebody point me to a document which explains how  
>the windows(Win2k/WinXP) login and logoff mechanism  
>works. I need to maintain a list of logged in user in the  
>domain and was wondering if I can do that by sniffing all  
>the packets on port 445 (SMB).

>

>thanks

>threqu

>.

>