

## Re: Identifying Windows O/S & SP

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-08/0315.html>

---

**From:** Ivan . (ivanhec\_at\_gmail.com)

**Date:** 08/25/05

Date: Thu, 25 Aug 2005 16:55:10 +1000

To: L3wD <l3wd@earthlink.net>

check out <http://www.thc.org/releases.php> they have a few tools. not sure about IDS evasion and the packet count

- THC-Amap
- THC-Vmap
- THC-Rut
- THC-Probe

check here too:

<http://www.networkintrusion.co.uk/osfp.htm>

finally try google

<http://www.google.com.au/search?q=daemon+fingerprinting&btnG=Search&hs=0v&hl=en&client=firefox-a&rls=org>

cheers

Ivan

On 8/25/05, L3wD <l3wd@earthlink.net> wrote:

> *I am looking for a method of correctly identifying Windows O/S Versions and Service Packs remotely. Here are my restrictions:*

- > *- Performed Remotely (not in same broadcast domain)*
- > *- No Admin Rights on Remote Box*
- > *- No Username/Password on Remote Box*
- > *- VERY Few Packets Generated (excluding TCP 3-way handshake)*
- > *- Ability to **\*\*AVOID\*\*** IDS Detection*

>

> *My preferences are for something that is command line based, and can be run from a Linux platform. I'll take something GUI based or Windows based if that is all there is. Multiple tools are fine, as long as the number of packets generated are very low.*

>

> *I've taken a look at Winfingerprint 0.6.2 with only the Win32 OS Version option selected, but it generates 70+ packets which is too loud for my purposes.*

>