

[TOOL] P0f – Passive OS Fingerprinting Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0033.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/12/04

To: list@securiteam.com

Date: 12 Jul 2004 16:46:30 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

P0f – Passive OS Fingerprinting Tool

SUMMARY

DETAILS

P0f v2 is a versatile passive OS fingerprinting tool. P0f can identify the operating system on:

- Machines that connect to your box (SYN mode),
- Machines you connect to (SYN+ACK mode),
- Machine you cannot connect to (RST+ mode),
- Machines whose communications you can observe.
- Analyze packets from tcpdump snapshot

P0f can also do many other tricks, and can detect or measure the following:

- Firewall presence or masquerading (useful for policy enforcement),
- The distance to the remote system and its uptime,
- Other guy's network hookup (DSL, OC3, avian carriers) and his ISP.

New features to version 2.0.4 include:

- RST+ACK (connection refused) fingerprinting
- Official SYN+ACK (outgoing connection) fingerprinting support
- Sophisticated masquerade / IP sharing detection algorithms
- TCP/IP stack bug dissector and fingerprinting support

Securiteam: [TOOL] P0f – Passive OS Fingerprinting Tool

- External query API for easier service integration
- Rudimentary fuzzy matching
- Cool supplementary utilities and ports

P0f is extremely useful in various security-related applications, including but not limited to traffic analysis, IDS, forensics, policy enforcement, pen testing, and low profile network reconnaissance.

More information, links to related or derived projects, and last but not least, source downloads, can be all found at:

<<http://lcamtuf.coredump.cx/p0f.shtml>>
<http://lcamtuf.coredump.cx/p0f.shtml>

You can get p0f v2 (2.0.4) by <<http://lcamtuf.coredump.cx/p0f.tgz>> clicking here. You can also try the most recent <<http://lcamtuf.coredump.cx/p0f-devel.tgz>> development snapshot

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lcamtuf@coredump.cx>> Michal Zalewski.

If you wish to stay up-to-date, you are welcome to the p0f project at:
<<http://www.freshmeat.net/projects/p0f/>>
<http://www.freshmeat.net/projects/p0f/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.