

[TOOL] RING, An Opensource OS Fingerprinting Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0081.html>

From: support@securiteam.com

Date: 04/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 20 Apr 2002 17:49:20 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

RING, An Opensource OS Fingerprinting Tool

DETAILS

RING is a new remote operating system fingerprinting tool based on temporal response analysis.

Carefully studying the way TCP works, especially some timer value inside the TCP stack, we have derived on a new technique for remote OS detection, based on temporal response analysis. The idea is quite simple: send a TCP SYN packet to an open port on a remote system, and listen the different answers (usually successive SYN/ACK packets). By measuring the number of response, the delay between retries, and the optional presence of a "RST" packet after a few answers, we can easily recognize some operating systems.

As a proof of concept, we also developed the standalone tool "RING" that will perform these testings and identifications, using a signature file.

ADDITIONAL INFORMATION

More information is available at:

<http://www.intranode.com/site/techno/techno_articles.htm>

http://www.intranode.com/site/techno/techno_articles.htm

Securiteam: [TOOL] RING, An Opensource OS Fingerprinting Tool

The tool can be downloaded from:

<<http://www.intranode.com/pdf/techno/ring-0.0.1.tar.gz>>
<http://www.intranode.com/site/techno/ring-0.0.1.tar.gz>

The full, 13 pages, white paper is available at:

<<http://www.intranode.com/pdf/techno/ring-full-paper.pdf>>
<http://www.intranode.com/pdf/techno/ring-full-paper.pdf>

This information has been provided by <mailto:mailto:Ring@intranode.com>
Ring.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Foundstone Fscan Format String Bug"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)