

OS fingerprinting technique

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-04/0031.html>

From: Franck Veysset (franck.veysset@intranode.com)

Date: 04/17/02

Date: Wed, 17 Apr 2002 19:25:14 +0200

From: Franck Veysset <franck.veysset@intranode.com>

To: "pen-test@securityfocus.com" <pen-test@securityfocus.com>

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. The nice thing is that it only required to send one packet on an open TCP port, which make this method really quiet.

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

More information is available at:

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

The open source tool can be downloaded from:

<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>

We will be very happy to get your feedback on this technique.

Feel free to contact us at: ring@intranode.com

Thanks,

-Franck

--

Franck Veysset -- <http://www.INTRANODE.com>
Intranode Software Technologies

SecurityFocus Penetration: OS fingerprinting technique

It is always possible to aglutenate multiple separate problems into a single complex interdependent solution. In most cases this is a bad idea. (RFC 1925)

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** Gary O'leary-Steele: "Debugging recent iis asp overflow"
- **Next in thread:** Franck Veysset: "Re: OS fingerprinting technique"
- **Reply:** Franck Veysset: "Re: OS fingerprinting technique"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]