

# [REVS] Analysis of Remote Active Operating System Fingerprinting Tools

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0004.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/03/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 3 Jun 2003 18:20:00 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Analysis of Remote Active Operating System Fingerprinting Tools

---

## SUMMARY

Many of today's tools are used for remote active operating system fingerprinting. They all have their own fingerprinting techniques. This paper gives an in-depth analysis of three such tools: Nmap, RINGv2, and Xprobe2. The purpose of the paper is to show how these tools work, and to understand the advantages and disadvantages they each offer.

## DETAILS

### Introduction:

Remote active operating system fingerprinting is the process of determining the identity of a remote host's operating system. This is done by actively sending packets to the remote host and analyzing the responses. Tools like Nmap and Xprobe2 take the responses and form a fingerprint that can be queried against a signature database of known operating systems. Learning which operating system is running on a remote host can be very valuable for both pentesters and black-hats. It is valuable because when vulnerabilities are found they are normally

## Securiteam: [REVS] Analysis of Remote Active Operating System Fingerprinting Tools

dependent on the OS version. Originally, determining the OS on the remote host was done by a technique known as "banner grabbing". Banner grabbing consists of either looking at the banner displayed when trying to connect to a service like ftp or by downloading a binary file like /bin/lis to determine what architecture it was built for. Eventually, more advanced techniques based on stack querying came about. Stack querying means to actively send packets to the network stack on the remote host and analyze the responses. This idea takes advantage of each OS vendor's network stack implementation. The first method to use stack querying was aimed at the TCP stack. It involves sending standard and non-standard TCP packets to the remote host and analyzing the responses. The next method was known as ISN (Initial Sequence Number) analysis<sup>1</sup>. This identifies the differences in the random number generators found in the TCP stack. Up until that point all of the stack querying methods were found by looking at the TCP protocol. Later the same year, researchers found a new method that used the ICMP protocol. The method is known as ICMP response analysis. It involves sending ICMP messages to the remote host and analyzing the responses. The newest method is called temporal response analysis. Like others, this method uses the TCP protocol. Temporal response analysis looks at the retransmission timeout (RTO) responses from a remote host.

This paper presents an in-depth analysis of three remote active OS fingerprinting tools. Ryan will be explaining how each of the different OS detection methods works in order to identify the OS running on the remote host. The goal of the paper is to show how the tools work, and to understand the advantages and disadvantages they each offer.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:ryan@packetwatch.net>> Ryan Spangler.

=====

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](mailto:list-unsubscribe@securiteam.com)

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