

[TOOL] IKE-Scan – VPN Scanning and Identification Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0105.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/24/05

To: list@securiteam.com

Date: 24 Feb 2005 17:09:04 +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>

IKE-Scan – VPN Scanning and Identification Tool

SUMMARY

DETAILS

The NTA Monitor VPN Fingerprinting tool (ike-scan) exploits transport characteristics in the Internet Key Exchange (IKE) service, the mechanism used by VPNs to establish a connection between a server and a remote client.

The ike-scan tool scans IP addresses for VPN servers by sending a specially crafted IKE packet to each host within a network. Most hosts running IKE will respond, identifying their presence. The tool then remains silent and monitors retransmission packets. These retransmission responses are recorded, displayed and matched against a known set of VPN product fingerprints.

Download Information:

Source distribution:

<<http://www.nta-monitor.com/ike-scan/download/ike-scan-1.7.tar.gz>>

ike-scan-1.7.tar.gz

The mentioned package will compile on UNIX and Linux systems as well as Windows systems with Cygwin. You will need a C compiler, the "make"

Securiteam: [TOOL] IKE-Scan – VPN Scanning and Identification Tool

utility and the appropriate system header files to compile ike-scan. It uses autoconf and automake, so compilation and installation is the normal /configure; make; make install process.

Windows binary:

<<http://www.nta-monitor.com/ike-scan/download/ike-scan-win32-1.7.zip>>
ike-scan-win32-1.7.zip

This mentioned package is a zip file containing a Win-32 binary version of ike-scan together with the Cygwin DLL which provides Posix support. It runs on Win-9x/ME, NT, 2000 and XP. The executable was produced by compiling the ike-scan source on a Windows system running Cygwin.

RPM packages: <<http://www.stearns.org/ike-scan/>>

<http://www.stearns.org/ike-scan/>

Thanks to Bill Stearns for producing the RPM packages.

Previous versions of ike-scan are available at:

<<http://www.nta-monitor.com/ike-scan/archive/>>

<http://www.nta-monitor.com/ike-scan/archive/>

If you specifically want an older version of the ike-scan software, then you can get it from here.

ADDITIONAL INFORMATION

To keep updated with the tool visit the project's homepage at:

<<http://www.nta-monitor.com/ike-scan/>>

<http://www.nta-monitor.com/ike-scan/>

=====

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.