

[TOOL] 4G8 – Packet Sniffer Over Switched Network

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0005.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/04/04

To: list@securiteam.com

Date: 4 Feb 2004 09:58:50 +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>

4G8 – Packet Sniffer Over Switched Network

DETAILS

<<http://forge.sourceforge.net>> 4G8 (Forge Gate) allows you to capture traffic from a third party in a switched environment at the expense of a slight increase in latency to that third party host. Utilizing ARP cache poisoning, packet capture and packet reconstruction techniques, 4G8 works with nearly all TCP, ICMP and UDP IPv4 traffic flows.

To run 4G8 you need to obtain the IP and MAC of the gateway, as well as the IP and MAC address of the target, both available by simply looking at the ARP table.

4G8 requires <<http://www.packetfactory.net/libnet>> libnet 1.1 or greater as well as <<http://tcpdump.org/>> libpcap. It has been successfully compiled and tested to run on FreeBSD, NetBSD, OpenBSD and Linux.

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://forge.sourceforge.net/downloads/4g8-0.9b.tgz>>

<http://forge.sourceforge.net/downloads/4g8-0.9b.tgz>

Securiteam: [TOOL] 4G8 – Packet Sniffer Over Switched Network

The information has been provided by <mailto:dounds@intrusense.com>
Darren Bound

=====

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.