

[TOOL] Skeeve – Software For Creating Cover Channel With ICMP Tunnel

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0116.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/25/05

To: list@securiteam.com

Date: 25 Jan 2005 18:44:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Skeeve – Software For Creating Cover Channel With ICMP Tunnel

SUMMARY

DETAILS

With this Proof Of Concept tool, you can create an ICMP tunnel between two computers, which may be located in different networks and separated by a Firewall. Skeeve utilizes ICMP packets and IP address spoofing technology to create a data channel in order to redirect TCP connections inside this channel.

How it works:

Skeeve creates an ICMP tunnel which is based on the use of a Bounce server.

This method relies upon the basic IP address spoofing technology. The Client of the tunnel is trying to send a packet to the Bounce server with an address of the destination Server as a source IP. The Bounce Server can replay this packet and forward it to the destination Server. By adding some payload to the packet, we can establish a covert communication channel between two computers without direct network interaction.

Securiteam: [TOOL] Skeeve – Software For Creating Cover Channel With ICMP Tunnel

Skeeve Client accepts TCP connections and works as a converter of the IP header (by changing protocol flag from TCP to ICMP echo_request|reply and making some other slight modifications). Skeeve Server is doing the reverse procedure and restores original IP header settings. Both parts are implemented in one C program as a Loadable Kernel module.

Download Information:

The tool can be obtained from:

<<http://gray-world.net/projects/skeeve/skeeve-1.0.tar.gz>>

<http://gray-world.net/projects/skeeve/skeeve-1.0.tar.gz>

ADDITIONAL INFORMATION

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

<http://gray-world.net/poc_skeeve.shtml>

http://gray-world.net/poc_skeeve.shtml

=====

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.