

[TOOL] Multispoof – Parallel Spoofing for Throughput Increase

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0009.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/02/05

To: list@securiteam.com

Date: 2 Nov 2005 09:33:23 +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>

Multispoof – Parallel Spoofing for Throughput Increase

SUMMARY

DETAILS

Multispoof is an application, which exploits weak, address based authentication very frequently implemented by ISPs in Ethernet networks. In such networks customers are identified with IP–MAC address pairs, and only those paying ISP are granted access to the Internet.

Multispoof uses IP and MAC spoofing to impersonate legitimate customers. The idea is not new, but multispoof does it in a smart way. As it impersonates only inactive customers, there is no address conflicts. And using multiple addresses in parallel in combination with load balancing allows to achieve much higher transfer rates.

It could be compared with download accelerating software, because higher throughput is achieved with multiple transmissions. The difference is that multispoof operates on layers 2 and 3 of the OSI model. In contrast, download accelerator uses multiple TCP streams – the fourth layer of OSI model.

Securiteam: [TOOL] Multispoof – Parallel Spoofing for Throughput Increase

Pawel Pokrywka has created multispoof as a software project for my M.Sc. thesis, so entire application (version 0.6.1) is documented quite precisely in there. If you read Polish, you can get my thesis in papers section on my page. I've spent entire chapter on spoofing detection and prevention techniques, so if you are an ISP, you may be interested too.

Features:

- * Accelerates throughput multiple times using parallel spoofing with load balancing
- * When aggressively used can fill up your ISP Internet link, so its great for testing maximal throughput of provider
- * IP and MAC spoofing
- * Only inactive addresses are used for spoofing. No address conflicts
- * Detection of active hosts performed with ARP scanning
- * Only addresses permitted to access external network (usually Internet) are used in spoofing process. Connectivity testing is easily configurable

ADDITIONAL INFORMATION

The information has been provided by <mailto:publicpp@gmail.com> Pawel Pokrywka.

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

<<http://multispoof.cryptonix.org/>> <http://multispoof.cryptonix.org/>

=====

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.