

[TOOL] Windows ARP Spoofer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0096.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/25/04

To: list@securiteam.com

Date: 25 Apr 2004 19:29:12 +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>

Windows ARP Spoofer

SUMMARY

DETAILS

The WinArpSpoofer program is a strong Windows-based ARP spoofer program with GUI based on the CBuildPacket class.

1.1 What is ARP spoofing?

ARP spoofing, also called ARP Cache poisoning is one of the hacking methods to spoof the contents of an ARP table on a remote computer on the LAN. Two addresses are needed for one computer to connect to other computer on an IP/Ether network. One address is the MAC address; the other is the IP address. A MAC address is used on a local area network before packets go out of the gateway; an IP address is used to surf the Internet through a gateway. There is a protocol that asks, "who has this MAC address" and answers the question; that is called ARP (Address Resolution Protocol). What the ARP asks the target address for sending is called the ARP Request or ARP who has, and the ARP that responds to the request is called the ARP Request or ARP who has. Although wrong information is inserted into ARP, the computer believes that the information of the ARP is valid and saves the information in own ARP table for a while. This is ARP spoofing.

1.3 CBuildPacket Class

CBuildPacket is a class that builds a WinArpSpoofer program. Its general purpose is to easily build a cooked packet throwing into the network. It is hard to understand and use existing libnet libraries and so forth in MS Visual.NET, so Gordon Ahn have newly designed this class.

The current version of the CBuildPacket class provides some methods for building and sending an ARP to the network. The future version of this class will provide many various types of network packets for building TCP, IP, icmp, and the like.

WinArpSpoofer has been built based on the current CBuildPacket class. It could pull and collect all packets without users' recognition. The current version, 0.1, has been built for spoofing ARP tables and actually forwarding packets, so we didn't consider a neat and convenient user interface. For the future, when upgrading, that point will be improved.

1.4 Features of WinArpSpoofer

Functions a