Global Information Assurance Certification Paper

“Real World ARP Spoofing”

Raúl Siles

August, 2003

*GIAC Certified **Incident Handler** (**GCIH**) Practical*
*(Version **2.1a** – Option 1: **Exploit in Action**)*

GIAC Certification Administrivia Version 2.5b

Abstract

This paper pretends to explore ARP, from its design and specifications point of view, the Internet RFCs, to its real world implementations, that is, how the operating systems analyzed behave. It explains how when dealing with ARP works, how to manipulate and configure the elements that constitute the ARP modules inside the TCP/IP stacks of different OS and how the protocol can be exposed from a security perspective.

It describes the security vulnerabilities that could be exploited using ARP to take control over the network traffic that flows between two systems in a Local Area Network, called “ARP spoofing or poisoning”, redirecting the traffic to a box owned by an attacker, and proposing some of the different advanced attacks that could be developed based on it.

The goal of this paper is trying to research and discover every small detail and component of the ARP protocol that will allow an attacker to get control over an unauthorized system, and to provide enough information for an administrator to be able to protect its network infrastructure.

The main motivation for this paper’s research was originated after more than two years of internal Penetration Testing over production environments, meaning by internal the situation where the security auditor plays the attacker’s role as an insider: employee, subcontractor, third-party support engineer or consultant…

Although the “ARP spoofing” technique is very simple in concept, in real world situations over heterogeneous networks, the obtained results are not always as expected, because both the operating system and network topology influences the way ARP behaves. Therefore, more information about how the ARP protocol and the “ARP spoofing” attack work should be obtained to be able to have as much control as possible over the ARP redirection games.

Layer 2 vulnerabilities are typically underestimated because they are associated with the attacker physically located next to the target system, but this is an incorrect approach. Once an attacker has got control over a system from outside, he is in the same situation as any insider.

From the author’s point of view, it is a must to understand every detail about how the ARP protocol and every implementation work and to play the potential role of an attacker to be prepared to defend the network against the different ARP attacks and their security vulnerabilities. For this reason sometimes this paper will analyze a specific aspect to reach the attacker’s goal, and sometimes it will focus on defending against the protocol exploitation.

Due to the fact that this is a very ambitious project, it will evolve and go into a deeper research of some areas in future versions, as, for example, covering additional operating systems and network traffic situations, such as those based on high availability solutions. The final goal will be to reach a similar work as the

one developed by Ofir Arkin about the ICMP protocol [OFIR1] but focusing on the ARP protocol. Sorry for being so ambitious, but using Ofir's paper as a reference is well worth.

This paper pretends to be the foundation of a future project called "**The SARP**: **The S**ecurity **A**RP **R**esearch **P**roject". My willing is to make this project available for the Internet community in the next few months.

To be able to agglutinate a huge knowledge around the ARP protocol, the Internet community should share information, so the new proposed ARP project could be a knowledge repository. Its main goal will be offering a database of the different ARP behaviours classified by OS. In the past there were similar projects, covering nearest information security areas, but they were unsuccessful [SSP1].

Some areas this project should include would be:

- Packet taxonomy: stimulus-response ARP traffic or how different OS respond to every possible ARP packet and how their ARP tables are populated, including big anomalies in packets.
- ARP table timeout behaviour: how each ARP timer work and how to configure it through OS kernel parameters.
- ARP bootstrap and shutdown times analysis.
- ARP behaviour when activating/deactivating network interfaces.
- ARP operating system fingerprinting.

Acknowledgements

"Mónica, there are no words to be able to express my feelings about you. Thanks so much for your support and help, and for reviewing this paper ;-)"

"To you, mum, to overcome any problem in this life with your energy and vitality"

"Marta, Jorge, David, thanks for your valuable contribution"

Revision

First version: **1.0** **August, 2003** – Author: Raúl Siles
Originally created for the SANS GIAC Practical paper needed to obtain the GCIH certification.

Table of Contents

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.