SAND2015-5877D

Exceptional service in the national interest

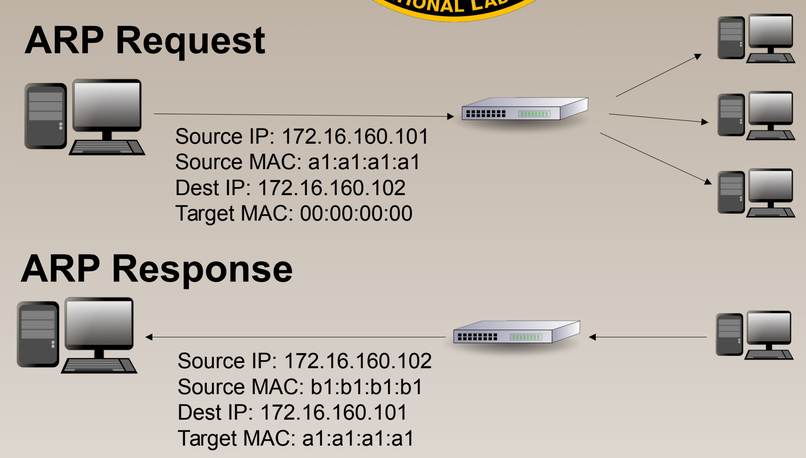
Sandia National Laboratories

cARP: Catching ARP Spoofing

Ethan Bowen, Pennsylvania State University, Cybersecurity, 2015
Apoorva Dornadula, UC Berkeley, Electrical Engineering Computer Science, 2017
Troy DeVries, Mentor, R&D S&E, Cybersecurity Research & Development
Organization: 8965

What is ARP?

Address Resolution Protocol, ARP, is a method of resolving a physical address to its Internet Protocol, IP address.



What is ARP Spoofing?

ARP Spoofing is a type of attack where the attacker poisons the target's ARP cache with it's own MAC address and a different IP address (ex. IP address of the gateway).

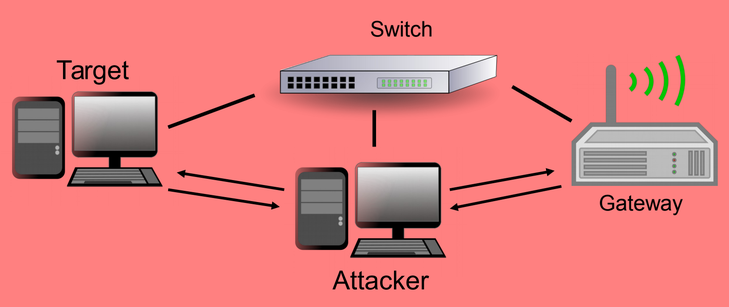
Our Tool

Our ARP detection tool is able to detect different variations of ARP Spoofing and can distinguish between a real attack and false positives.

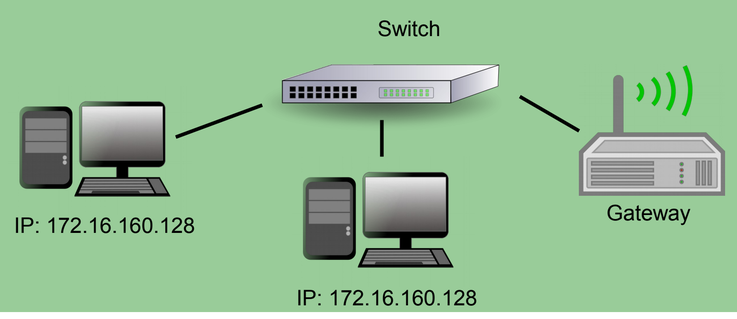
	cARP	Arpwatch
Checks False Positives	✓	✗
Handling VLAN Tags	✓	✗
Effective Alerting	✓	✗
Identifies Attacker	✓	✗
Real Time Analysis	✗ (not yet)	✓

Cases

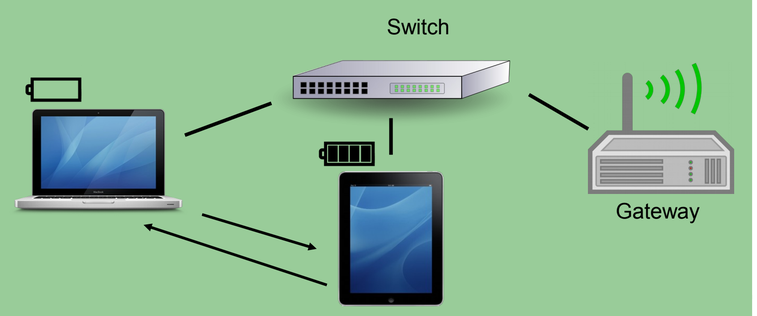
Two Way Spoofing



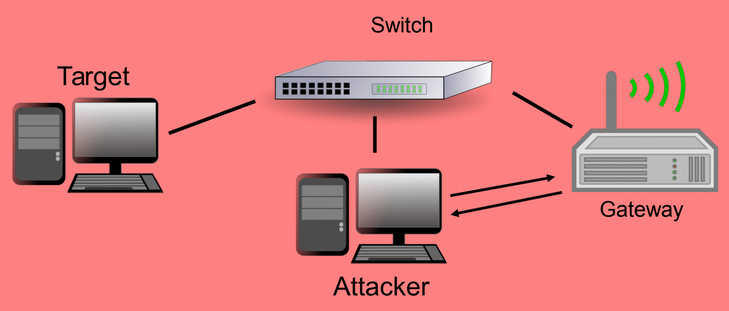
IP Conflict



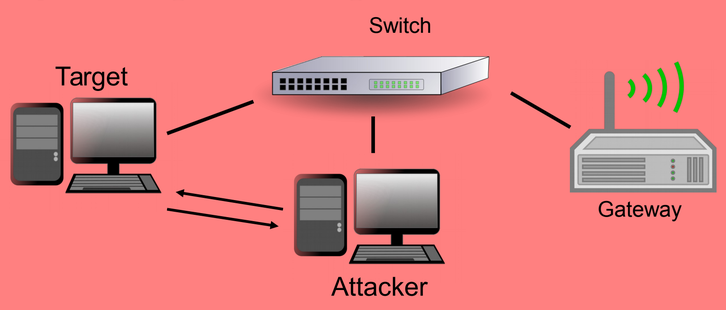
Apple Power Saving Feature



Spoofing the Gateway

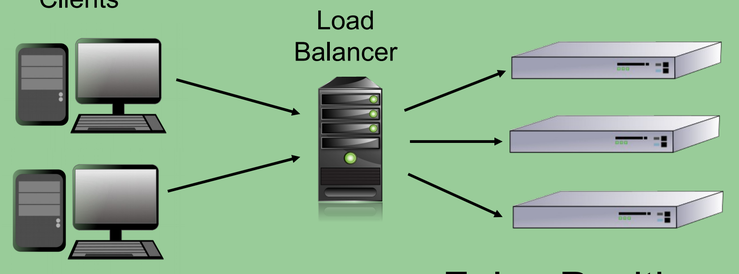


Spoofing the Target



Real Spoofing

Load Balancers



False Positives

How it Works

The tool detects ARP Spoofing by analyzing packet traffic using a Python library called Scapy. When a physical address is matched with two different IP addresses, it is run through multiple checks before an alert is sent.

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2011-XXXXP