ARP spoofing

From Wikipedia, the free encyclopedia

A successful ARP spoofing attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack.

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

The attack can only be used on networks that make use of the Address Resolution Protocol (ARP), and is limited to local network segments.

Contents

1. Vulnerabilities of the Address Resolution Protocol
2. Anatomy of an ARP spoofing attack
3. Defences
3.1 Static ARP entries
3.2 ARP spoofing detection software
3.3 OS security
4. Legitimate usage
5. See also
5.1 Tools
5.1.1 Defence
5.1.2 Spoofing
6. References
7. External links

Vulnerabilities of the Address Resolution Protocol

The Address Resolution Protocol (ARP) is a widely used protocol for resolving network layer addresses into link layer addresses.

When an Internet Protocol (IP) datagram is sent from one host to another on a local area network, the destination IP address must be converted into a MAC address for transmission via the data link layer. When another host's IP address is known, and its MAC address is needed, a broadcast packet is sent out on the local network. This packet is known as an ARP request. The destination machine with the IP in the ARP request then responds with an ARP reply, which contains the MAC address for that IP.

ARP is a stateless protocol. Network hosts will automatically cache any ARP replies they receive, regardless of whether or not they requested them. Even ARP entries which have not yet expired will be overwritten when a new ARP reply packet is received. There is no method in the ARP protocol by which a host can authenticate the peer from which the packet originated. This behaviour is the vulnerability which allows ARP spoofing to occur.

Anatomy of an ARP spoofing attack

The basic principle behind ARP spoofing is to exploit the above mentioned vulnerabilities in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN.

Generally, the goal of the attack is to associate the attacker's MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's MAC instead. The attacker could then choose to:

- Inspect the packets, and forward the traffic to the actual default gateway (interception)
- Modify the data before forwarding it (man-in-the-middle attack).
- Launch a denial-of-service attack by causing some or all of the packets on the network to be dropped

Defences

Static ARP entries

IP-to-MAC mappings in the local ARP cache can be statically defined, and then hosts can be directed to ignore all ARP reply packets.[5] While static entries provide perfect security against spoofing if the operating systems handles them correctly, they result in quadratic maintenance efforts as IP-MAC mappings of all machines in the network have to be distributed to all other machines.

ARP spoofing detection software

Software that detects ARP spoofing generally relies on some form of certification or cross-checking of ARP responses. Uncertified ARP responses are then blocked. These techniques may be integrated with the DHCP server so that both dynamic and static IP addresses are certified. This capability may be implemented in individual hosts or may be integrated into Ethernet switches or other network equipment. The existence of multiple IP addresses associated with a single MAC address may indicate an ARP spoof attack, although there are legitimate uses of such a configuration. In a more passive approach a device listens for ARP replies on a network, and sends a notification via email when an ARP entry changes.

OS security

Operating systems react differently, e.g. Linux ignores unsolicited replies, but on the other hand uses seen requests from other machines to update its cache. Solaris only accepts updates on entries after a timeout. In Microsoft Windows, the behaviour of the ARP cache can be configured through several registry entries under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, ArpCacheLife, ArpCacheMinReferenceLife, ArpUseEtherSNAP, ArpTRSingleRoute, ArpAlwaysSourceRoute, ArpRetryCount.

AntiARP also provides Windows-based spoofing prevention at the kernel level. ArpStar is a Linux module for kernel 2.6 and Linksys routers, which drops invalid packets that violate mapping, and contains an option to re-poison/heal.

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. This only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n*n) ARP caches that have to be configured.

Legitimate usage

ARP spoofing can also be used for legitimate purposes. For instance, network registration tools may redirect unregistered hosts to a signup page before allowing them full access to the network. This technique is used in hotels and other semi-public networks to allow traveling laptop users to access the Internet through a device known as a head end processor (HEP).

ARP spoofing can also be used to implement redundancy of network services. A backup server may use ARP spoofing to take over for a defective server and transparently offer redundancy.

ARP spoofing is often used by developers to debug IP traffic between two hosts when a switch is in use.

Tools

Defense

- anti-arpspoof
- Arpwatch
- ArpON: Portable handler daemon for securing ARP against spoofing, cache poisoning or poison routing attacks in static, dynamic and hybrid networks.
- Antidote: Linux daemon, monitors mappings, unusually large number of ARP packets.
- Arp_Antidote: Linux Kernel Patch for 2.4.18 - 2.4.20, watches mappings, can define action to take when.
- ArpGuard: ArpGuard protects your Mac by keeping an eye on your Internet network.
- Arpalert: Predefined list of allowed MAC addresses, alert if MAC that is not in list.
- Arpwatch/ArpwatchNG/Winarpwatch: Keep mappings of IP-MAC pairs, report changes via Syslog, Email.
- Prelude IDS: ArpSpoof plugin, basic checks on addresses.
- Snort: Snort preprocessor Arpspoof, performs basic checks on addresses
- XArp: Advanced ARP spoofing detection, active probing and passive checks. Two user interfaces: normal view with predefined security levels, pro view with per-interface configuration of detection modules and active validation. Windows and Linux, GUI-based.

Spoofing

Some of the tools that can be used to carry out ARP spoofing attacks:

- Arpspoof (part of the DSniff suite of tools)
- Arpoison
- Ettercap
- Cain&Abel
- Seringe
- ARP-FILLUP -V0.1
- arp-sk -v0.0.15
- ARPOc -v1.13
- arpalert -v0.3.2
- arping -v2.04
- arpmitm -v0.2[

- arpoison -v0.5
- ArpSpyX -v1.1
- ArpToXin -v 1.0
- SwitchSniffer
- APE - ARP Poisoning Engine

Name	OS	GUI	Free	Protection	Per interface	Active/passive
Agnitum Outpost FW	Windows	Yes	No	Yes	No	passive
AntiARP	Windows	Yes	No	Yes	No	active+passive
Antidote	Linux	No	Yes	No	?	passive
Arp_Antidote	Linux	No	Yes	No	?	passive
Arpalert	Linux	No	Yes	No	Yes	passive
ArpON	Linux/Mac/BSD	No	Yes	Yes	Yes	active+passive
ArpGuard	Mac	Yes	No	Yes	Yes	active+passive
ArpStar	Linux	No	Yes	Yes	?	passive
Arpwatch	Linux	No	Yes	No	?	passive
ArpwatchNG	Linux	No	Yes	No	No	passive
Colasoft Capsa	Windows	Yes	No	No	Yes	no detection, only analysis with manual inspection
remarp	Linux	No	Yes	No	No	passive
Snort	Windows/Linux	No	Yes	No	Yes	passive
Winarpwatch	Windows	No	Yes	No	No	passive
XArp	Windows, Linux	Yes	Yes (+pro version)	Yes (Linux, pro)	Yes	active + passive
Seconfig XP	Windows 2000/XP/2003 only	Yes	Yes	Yes	No	only activates protection built-in some versions of Windows