

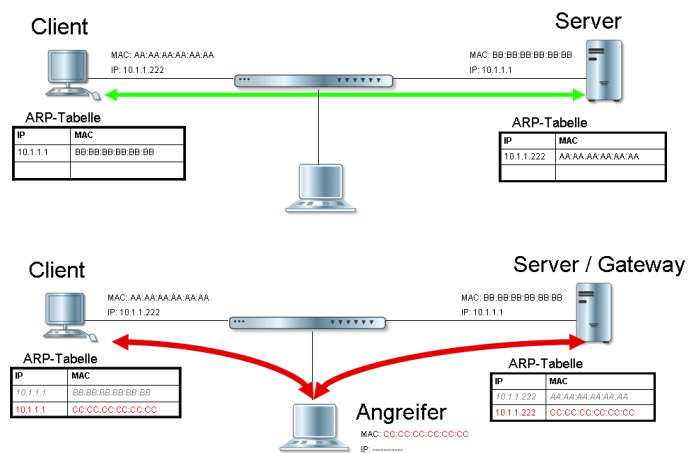
macmon advanced security Option

Schutz vor ARP-Angriffen

Das gezielte Senden von gefälschten ARP-Paketen wird beim ARP-Spoofing oder auch ARP-Poisoning dazu benutzt, um den Datenverkehr zwischen zwei Hosts in einem Datenetz abzuheören oder zu manipulieren.

Die advanced security Option schützt vor solchen Man-In-The-Middle Angriffen, indem es ARP-Veränderungen erkennt und auf diese über die Ereignisverarbeitung reagieren kann. Dies erfolgt zentral vom macmon-Server aus, ohne Sensoren in den einzelnen Netzwerksegmenten zu platzieren.

Die macmon advanced security Option bietet verschiedene Ansätze um ARP-Manipulationen zu erkennen und zu verhindern:



Vorgaben in der Referenzliste

ARP- Informationen werden mit einer internen, manuell zu pflegenden Referenzliste verglichen. Kommt es zu Abweichungen von diesen Vorgaben, wird das Ereignis „**mac_ip_mismatch**“ ausgelöst. macmon erkennt, an welcher Stelle vorgegebene mac→ip - Zuordnungen manipuliert wurden und kann Gegenmaßnahmen einleiten.

Veränderungsüberwachung

Da die mac→ip Zuordnungen, die in den ARP-Tabellen gehalten werden, selten wechseln, überwacht macmon diese Zuordnungen auf Veränderungen, indem es aktuelle Messdaten mit älteren vergleicht. Ergeben sich hier innerhalb eines vorher als kritisch definierten Zeitraums Abweichungen in den mac→ip - Zuordnungen erzeugt macmon das Event „**arp_spoofing**“ und es können über das Regelwerk automatisch Gegenmaßnahmen eingeleitet werden.

macmon advanced security Option

DHCP-Import

Werden in einer Infrastruktur DHCP-Server mit kurzen Lease-Zeiten verwendet, ist das Verfahren, ARP- Poisoning über ARP- Veränderungen in einem vorher festgelegten Veränderungsintervall zu erkennen, unter Umständen unzuverlässig.

Ist das Überwachungsintervall zu klein gewählt, können gewollte Veränderungen für Angriffe gehalten werden, ist es zu groß, werden Angriffe unter Umständen nicht erkannt.

Mit dem DHCP-Import erhält macmon die Möglichkeit die Konfigurationsdaten von DHCP-Servern einzulesen. macmon kennt so für alle über DHCP gesteuerten Systeme die fest, automatisch und dynamisch zugeordneten IP-Adressen mit ihren Gültigkeitszeiten (Lease-Time) und hat somit eine valide Referenzliste für die Bewertung der ARP-Daten.

Stellt macmon nun Abweichungen fest, wird ein „**mac_ip_mismatch**“-Ereignis ausgelöst, und es können über das Regelwerk gesteuert automatische Schutzmaßnahmen ausgelöst werden.

Auch die im DHCP-Server vorhandenen Namens-Informationen werden eingelesen und dem macmon- Berichtswesen zur Verfügung gestellt.

Schnittstelle

Das Auslesen der Daten erfolgt wahlweise über Skripte oder über einen https-Upload. Zum Betrieb der Schnittstelle müssen neben einem Skript keine Zusatztools auf dem jeweiligen DHCP-Server installiert werden.

Das Auslesen der Daten erfolgt zyklisch in frei definierbaren Intervallen.

Unterstützte Systeme

Die Option enthält Connectoren zu den DHCP-Servern von Windows (2000, 2003) und von Novell Netware.

Der Connector für Linux ist in Vorbereitung.

Die macmon advanced security Option setzt eine aktuelle Version von macmon voraus.