ARP SPOOFING DETECTED

DESCRIPTION:

ARP cache poisoning is the act of introducing a specious IP-to-Ethernet address mapping in another hostâ€™s ARP cache. This results in diversion of traffic, either to a different host on the LAN or no host at all. ARP spoofing, also known as the "Man In The Middle" attack, can thus be used to compromise the subnet. Even though ARP spoofing is possible only on a LAN it is still a security breach.

PREVENTION METHODS:

Static ARP Tables

Itâ€™s possible to statically map all the MAC addresses in a network to their rightful IP addresses. This is highly effective in preventing ARP Poisoning attacks but adds a tremendous administrative burden. Any change to the network will require manual updates of the ARP tables across all hosts, making static ARP tables unfeasible for most larger organizations. Still, in situations where security is crucial, carving out a separate network segment where static ARP tables are used can help to protect critical information.

Switch Security

Most managed Ethernet switches sport features designed to mitigate ARP Poisoning attacks. Typically known as Dynamic ARP Inspection (DAI), these features evaluate the validity of each ARP message and drop packets that appear suspicious or malicious. DAI can also typically be configured to limit the rate at which ARP messages can pass through the switch, effectively preventing DoS attacks.

DAI and similar features were once exclusive to high-end networking gear, but are now common on almost all business-grade switches, including those found in smaller businesses. Itâ€™s generally considered a best practice to enable DAI on all ports except those connected to other switches. The feature does not introduce a significant performance impact but may need to be enabled in conjunction with other features like DHCP

Snooping.

Enabling Port Security on a switch can also help mitigate ARP Cache Poisoning attacks. Port Security can be configured to allow only a single MAC address on a switch port, depriving an attacker the chance to maliciously assume multiple network identities.

Physical Security

Properly controlling physical access to your place of business can help mitigate ARP Poisoning attacks. ARP messages are not routed beyond the boundaries of the local network, so would-be attackers must be in physical proximity to the victim network or already have control of a machine on the network. Note that in the case of wireless networks, proximity doesnâ€™t necessarily mean the attacker needs direct physical access; a signal extends to a street or parking lot may be sufficient. Whether wired or wireless, the use of technology like 802.1x can ensure that only trusted and/or managed devices can connect to the network.

Network Isolation

As stated previously, ARP messages donâ€™t travel beyond the local subnet. This means that a well-segmented network may be less susceptible to ARP cache poisoning overall, as an attack in one subnet cannot impact devices in another. Concentrating important resources in a dedicated network segment where enhanced security is present can greatly diminish the potential impact of an ARP Poisoning attack.

Encryption

While encryption wonâ€™t actually prevent an ARP attack from occurring, it can mitigate the potential damage. A popular use of MiTM attacks was to capture login credentials that were once commonly transmitted in plain text. With the widespread use of SSL/TLS encryption on the web, this type of attack has become more difficult. The threat actor can still intercept the traffic, but canâ€™t do anything with it in its encrypted form.