ARP スプーフィングインスペクタ

ARP スプーフィングインスペクタの概要

タイプ	インスペクタ（ネットワーク）
使用方法	検査
インスタンス タイプ	単一
その他のインスペクタが必要	なし
有効	`true`

Address Resolution Protocol（ARP）は、アドレス解決のために単一のネットワーク内で使用されるステートレス通信プロトコルです。要求と応答を交換する場合、ARP はホスト間の認証を行いません。

ARP スプーフィングは、ローカルエリアネットワーク（LAN）内で ARP を使用する中間者攻撃の一種です。攻撃者は、特定のホストのMedia Access Control（MAC）アドレス宛てのメッセージを傍受することで、ホストへの通信を変更します。

`arp_spoof` インスペクタは、ARP パケットを分析し、ユニキャスト ARP 要求を検出します。ARP キャッシュ上書き攻撃を検出するために、ARP スプーフィングインスペクタは、一貫性のないイーサネットから IP へのマッピングを識別します。

有効になっている場合、`arp_spoof` インスペクタは次のことを行います。

- イーサネットアドレスと ARP パケット内のアドレスを検査します。不整合が発生すると、インスペクタはルール 112:2 またはルール 112:3 を使用してアラートを生成し、インライン展開で問題のあるパケットをドロップします。

- ユニキャスト ARP 要求を確認します。ユニキャスト ARP 要求が検出されると、インスペクタはルール 112:1 を使用してアラートを生成し、インライン展開で問題のあるパケットをドロップします。
- `hosts[]` パラメータが指定されている場合、インスペクタはその情報を使用して ARP キャッシュ上書き攻撃を検出します。このような攻撃が検出された場合、インスペクタはルール 112:4 を使用してアラートを生成し、インライン展開で問題のあるパケットをドロップします。

ARP スプーフィングインスペクタのパラメータ

`arp_spoof` インスペクタは、Secure Firewall Management Center Web インターフェイスにデフォルト設定パラメータ値を提供しません。

ARP スプーフィングインスペクタのルール

`arp_spoof` インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *1: ARP* スプーフィングインスペクタのルール

GID:SID	ルール メッセージ
112:1	ユニキャスト ARP 要求（unicast ARP request）
112:2	送信元のイーサネット/ARP 不一致要求（ethernet/ARP mismatch request for source）
112:3	接続先に対するイーサネット/ARP 不一致要求（ethernet/ARP mismatch request for destination）
112:4	ARP キャッシュの上書き攻撃が試行された（attempted ARP cache overwrite attack）

ARPスプーフィングインスペクタの侵入ルールのオプション

`arp_spoof` インスペクタには、侵入ルールオプションはありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。