ストリーム ICMP インスペクタ

ストリーム ICMP インスペクタの概要

タイプ	インスペクタ（ストリーム）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	なし
有効	`true`

Internet Control Message Protocol（ICMP）は、ネットワーク ユーティリティ アプリケーションやネットワークデバイスで使用されるネットワーク層プロトコルです。ICMP は、診断情報とエラー情報を送信して、IP ホスト間の通信が成功したか、または失敗したかを識別します。ICMP メッセージには、ヘッダーセクションとデータセクションが含まれます。

ICMP は、他のフローに関する情報を伝達します。リアセンブルが必要なデータは伝送せず、ターゲットベースのバインドも必要ありません。

`stream_icmp` インスペクタは、ICMP フロートラッキングを定義します。ping の場合、インスペクタは、ICMP ヘッダーの送信元および接続先の IP アドレスフィールドとポートフィールドを介して基本的なフロートラッキングを実行します。到達不能な接続先の場合、インスペクタは元の IP アドレスと転送ポートを分析し、セッションの状態を更新します。`port_scan` インスペクタは、到達不能なホストとポートが使用可能な場合は、それらを使用できます。

ストリーム ICMP インスペクタを設定するためのベストプラクティス

stream_icmp インスペクタを設定する場合は、次のベストプラクティスを考慮してください。

- ホストまたはネットワークに適用するセッションタイムアウトごとに stream_icmp インスペクタを作成します。stream_icmp インスペクタは、session_timeout を binder インスペクタで定義されている ICMP ホストまたはネットワークに関連付けます。

  同じネットワーク分析ポリシー（NAP）に複数のバージョンの stream_icmp インスペクタを含めることができます。

ストリーム ICMP インスペクタのパラメータ

session_timeout

stream_icmp インスペクタが状態テーブルの非アクティブな ICMP ストリームを保持する秒数を指定します。Snort が同じフローキーを持つ ICMP データグラムを次に 検出すると、以前のフローのセッションタイムアウトが期限切れになっているかどうかが確認されます。タイムアウトの期限が切れると、Snort はフローを閉じて新しいフローを開始します。Snort は、基本のストリーム設定に関連付けられた古いフローを確認します。

型：整数

有効な範囲：0 ～ 2,147,483,647 (max31)

デフォルト値：60

ストリーム ICMP インスペクタのルール

stream_icmp インスペクタには、関連付けられたルールはありません。

ストリーム ICMP インスペクタの侵入ルールのオプション

stream_icmp インスペクタには侵入ルールの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。