ポートスキャンインスペクタ

ポートスキャンインスペクタの概要

タイプ	インスペクタ（プローブ）
使用方法	グローバル
インスタンス タイプ	グローバル
その他のインスペクタが必要	なし
有効	false

ポートスキャンとは、攻撃者が攻撃の準備段階としてよく使用する、ネットワーク調査の形式です。ポートスキャンでは、攻撃者はターゲットホスト上のネットワークプロトコルとサービスをプローブするように設計されたパケットを送信します。攻撃者は、ホストが応答で送信したパケットを確認することで、ホスト上のどのポートが開かれているか、または開かれているポートでどのアプリケーションプロトコルが実行されているかを直接あるいは推論によって判断できます。

ポートスキャン自体は攻撃の証拠になりません。ネットワーク上の正当なユーザーが、攻撃者が使用するのと同様のポートスキャン技術を使用している可能性があります。

`port_scan` インスペクタは、4 種類のポートスキャンを検出し、TCP、UDP、ICMP、および IP プロトコルでの接続試行をモニタします。`port_scan` インスペクタは、アクティビティのパターンを検出することで、どのポートが悪意のあるポートであるかを判断するのに役立ちます。

表 *1:* ポートスキャンプロトコルのタイプ

プロトコル	説明
TCP	TCP プローブを検出します。たとえば、SYN スキャン、ACK スキャン、TCP connect() スキャン、および（Xmas tree、FIN、NULL）といった異常なフラグを組み合わせたスキャンなどです。
UDP	ゼロバイト UDP パケットなどの UDP プローブを検出します。
ICMP	ICMP エコー要求（ping）を検出します。
IP	IP プロトコル スキャンを検出します。Snort は、開いているポートを探すのではなく、ターゲットホストでサポートされている IP プロトコルを検索します。

一般に、ターゲットホストの数、スキャン側ホストの数、およびスキャン対象のポートの数に応じて、ポートスキャンは 4 つのタイプに分けられます。

表 *2:* ポートスキャン タイプ

タイプ	説明
ポートスキャン	攻撃者が少数のホストを使用して、1 つの対象ホスト上で複数のポートをスキャンする 1 対 1 ポートスキャン。 1 対 1 ポートスキャンには次のような特徴があります。 • 少数のホストを使用してスキャン • 単一のホストをスキャン • 多数のポートをスキャン ポートスキャンでは、TCP、UDP、および IP のポートスキャンが検出されます。
ポートスイープ	攻撃者が少数のホストを使用して、複数の対象ホスト上で 1 つのポートをスキャンする 1 対多のポートスイープ。 ポートスイープには次のような特徴があります。 • 少数のホストを使用してスキャン • 多数のホストをスキャン • 少数の固有のポートをスキャン ポートスイープでは、TCP、UDP、ICMP、および IP のポートスイープが検出されます。

タイプ	説明
デコイ ポートスキャン	攻撃者がスプーフィングされた送信元IPアドレスと実際にスキャンされたIPアドレスとを組み合わせた1対1ポートスキャン。 デコイポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 少数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン デコイポートスイープでは、TCP、UDP、およびIPのプロトコルポートスキャンが検出されます。
分散型ポートスキャン	複数のホストが開いているポストに対して1つのホストをクエリする多対1のポートスキャン。 分散型ポートスキャンには次のような特徴があります。 • 多数のホストを使用してスキャン • 多数のポートを一度だけスキャン • 単一（または少数）のホストをスキャン 分散型ポートスキャンでは、TCP、UDP、およびIPのプロトコルポートスキャンが検出されます。

ポートスキャン感度のレベル

`port_scan` インスペクタは、3つのレベルのデフォルトのスキャン感度を備えています。

- default_low_port_scan
- default_med_port_scan
- default_high_port_scan

さまざまなフィルタを使用して、追加のスキャン感度レベルを構成できます。

- scans
- rejects
- nets
- ports

`port_scan` インスペクタは、プローブされたホストから否定応答を収集することで、プローブについて学習します。たとえば、Webクライアントが TCP を使用して Web サーバーに接続している場合、そのクライアントは Web サーバーがポート 80 でリスニングしていると想定できます。ただし、攻撃者がサーバーをプローブする場合、そのサーバーが Web サービスを提供

するかどうかを攻撃者は事前に知っているわけではありません。port_scan インスペクタは否定応答（つまり、ICMP 到達不能または TCP RST パケット）を検出すると、その応答を潜在的ポートスキャンとして記録します。否定応答をフィルタリングするデバイス（ファイアウォールやルータなど）の向こう側にターゲットホストがある場合、このプロセスはさらに困難になります。この場合、port_scan インスペクタは、選択した機密レベルに基づいてフィルタ処理されたポートスキャンイベントを生成することができます。

ポートスキャンインスペクタを設定するためのベストプラクティス

ポートスキャンの検出を最適化するには、port_scan インスペクタをネットワークに合わせて調整することをお勧めします。

- watch_ip パラメータは慎重に設定してください。watch_ip パラメータは、port_scan インスペクタがネットワーク上で非常にアクティブな正当なホストをフィルタ処理するのに役立ちます。最も一般的な例には、NAT IP、DNS キャッシュサーバー、syslog サーバー、および nfs サーバーがあります。
- port_scan インスペクタが生成する可能性のある誤検知のほとんどは、フィルター処理済みスキャンの alert タイプです。alert タイプは、特定の期間にホストが過度にアクティブであったことを示している場合があります。ホストがフィルタ処理済みスキャンの alert タイプを継続的に生成する場合は、ホストを ignore_scanners リストに追加するか、スキャン感度のレベルを低くします。
- プライオリティカウント、接続数、IP 数、ポート数、IP 範囲、およびポート範囲を使用して、誤検知を特定します。 誤検知を判断する最も簡単な方法は、単純な比率の推定です。次に、推定する比率と、誤検知ではなく正当なスキャンを示す関連値のリストを示します。
  - 接続数/IP 数：この比率は、IP ごとの接続の推定平均を示します。ポートスキャンの場合、この比率は高くなります。ポートスイープの場合、この比率は低くなります。
  - ポート数/IP 数：この比率は、IP ごとに接続されているポートの推定平均を示します。ポートスキャンの場合はこの比率が高くなり、スキャンされたホストのポートは少数の IP で接続されていたことを示します。ポートスイープの場合はこの比率が低くなり、スキャンするホストは少数のポートに接続していても、多くのホスト上で接続していることを示します。
  - 接続数/ポート数：この比率は、ポートごとの接続の推定平均を示します。ポートスキャンの場合、この比率は低くなります。これは、各接続が異なるポートに対して行われたことを示しています。ポートスイープの場合、この比率は高くなります。これは、同じポートに多くの接続があったことを示しています。

  プライオリティカウントが高いほど、実際のポートスキャンまたはポートスイープである可能性が高くなります（ホストがファイアウォールで管理されている場合を除く）。

- ポートスキャンを検出できない場合は、スキャン感度レベルを下げることができます。スキャン感度レベルを高くすることで、最適な保護が得られます。スキャン感度レベルが低いと、エラー応答に基づいてアラートのみが生成され、フィルタ処理済みのスキャンは捕捉されません。スキャン感度レベルが低い場合のエラー応答は、ポートスキャンを示している可能性があり、感度レベルが低いことによって生成されるアラートは非常に正確であり、必要とする調整は最小限ですみます。フィルタ処理されたスキャンまたは感度レベルの高いスキャンには、誤検知の傾向があります。

ポートスキャンインスペクタのパラメータ

memcap

最大トラッカーメモリをバイト単位で指定します。

型：整数

有効な範囲：1024 〜 9,007,199,254,740,992 (maxSZ)

デフォルト値：10,485,760

protos

モニタするプロトコルを指定します。プロトコルの省略形の文字列を入力します。複数のプロトコルを指定するには、各プロトコルの省略形をスペースで区切ります。

型：文字列

有効な値：tcp、udp、icmp、ip、all

デフォルト値：all

scan_types

調べるポートスキャンのタイプを指定します。プロトコルの省略形の文字列を入力します。複数のプロトコルを指定するには、各プロトコル文字列をスペースで区切ります。

型：文字列

有効な値：portscan、portsweep、decoy_portscan、distributed_portscan、all

デフォルト値：all

watch_ip

監視するオプションのポートを持つ CIDR ブロックと IP のリストを指定します。

watch_ip が定義されていない場合、port_scan インスペクタはすべてのネットワークトラフィックを確認します。

型：文字列

有効な値：CIDR または IP アドレス、CIDR または IP アドレスのリスト

デフォルト値：なし

alert_all

確立したウィンドウ内のしきい値を超えるすべてのイベントについてアラートを生成するかどうかを指定します。`alert_all` が `false` に設定されている場合、`port_scan` インスペクタは、ウィンドウ内のしきい値を超える最初のイベントについてのみアラートを生成します。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

include_midstream

オプションのポートが含まれた CIDR をリストするかどうかを指定します。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

tcp_decoy.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：`0` ～ `65535`

デフォルト値：`15`

tcp_decoy.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：`0` ～ `65535`

デフォルト値：`25`

tcp_decoy.scan

スキャンの試行回数を指定します。

型：整数

有効な範囲：`0` ～ `65535`

デフォルト値：`100`

tcp_decoy.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_dist.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

tcp_dist.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_dist.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

tcp_dist.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_ports.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

tcp_ports.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_ports.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

tcp_ports.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_sweep.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

tcp_sweep.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

tcp_sweep.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

tcp_sweep.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_decoy.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

udp_decoy.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_decoy.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

udp_decoy.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_dist.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

udp_dist.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_dist.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

udp_dist.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_ports.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

udp_ports.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_ports.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

udp_ports.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_sweep.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

udp_sweep.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

udp_sweep.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

udp_sweep.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_decoy.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

ip_decoy.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_decoy.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

ip_decoy.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_dist.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

ip_dist.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_dist.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

ip_dist.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_sweep.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

ip_sweep.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_sweep.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

ip_sweep.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_proto.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

ip_proto.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

ip_proto.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

ip_proto.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

icmp_sweep.rejects

否定応答のスキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：15

icmp_sweep.ports

以前の試行からポート（またはプロトコル）が変更された回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：25

icmp_sweep.scans

スキャンの試行回数を指定します。

型：整数

有効な範囲：0 〜 65535

デフォルト値：100

icmp_sweep.nets

以前の試行からアドレスが変更された回数を指定します。

型：整数

有効な範囲：0 ～ 65535

デフォルト値：25

tcp_window

Transmission Control Protocol（TCP）スキャンの検出間隔を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

udp_window

User Datagram Protocol（UDP）スキャンの検出間隔を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

ip_window

Internet Protocol（IP）スキャンの検出間隔を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

icmp_window

Internet Control Message Protocol（ICMP）スキャンの検出間隔を指定します。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

ポートスキャンインスペクタのルール

port_scan インスペクタ 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 *3:* ポートスキャンインスペクタのルール

GID:SID	ルール メッセージ
122:1	TCP ポートスキャン（TCP portscan）
122:2	TCP デコイポートスキャン（TCP decoy portscan）
122:3	TCP ポートスイープ（TCP portsweep）
122:4	TCP 分散型ポートスキャン（TCP distributed portscan）
122:5	TCP フィルタ処理済みポートスキャン（TCP filtered portscan）
122:6	TCP フィルタ処理済みデコイポートスキャン（TCP filtered decoy portscan）
122:7	TCP フィルタ処理済みポートスイープ（TCP filtered portsweep）
122:8	TCP フィルタ処理済み分散型ポートスキャン（TCP filtered distributed portscan）
122:9	IP プロトコルスキャン（IP protocol scan）
122:10	IP デコイプロトコルスキャン（IP decoy protocol scan）
122:11	IP プロトコルスイープ（IP protocol sweep）
122:12	IP 分散型プロトコルスキャン（IP distributed protocol scan）
122:13	IP フィルタ処理済みプロトコルスキャン（IP filtered protocol scan）
122:14	IP フィルタ処理済みデコイプロトコルスキャン（IP filtered decoy protocol scan）
122:15	IP フィルタ処理済みプロトコルスイープ（IP filtered protocol sweep）
122:16	IP フィルタ処理済み分散型プロトコルスキャン（IP filtered distributed protocol scan）
122:17	UDP ポートスキャン（UDP portscan）
122:18	UDP デコイポートスキャン（UDP decoy portscan）
122:19	UDP ポートスイープ（UDP portsweep）
122:20	UDP 分散型ポートスキャン（UDP distributed portscan）
122:21	UDP フィルタ処理済みポートスキャン（UDP filtered portscan）
122:22	UDP フィルタ処理済みデコイポートスキャン（UDP filtered decoy portscan）
122:23	UDP フィルタ処理済みポートスイープ（UDP filtered portsweep）

GID:SID	ルール メッセージ
122:24	UDP フィルタ処理済み分散型ポートスキャン（UDP filtered distributed portscan）
122:25	ICMP スイープ（ICMP sweep）
122:26	ICMP フィルタ処理済みスイープ（ICMP filtered sweep）
122:27	オープンポート（open port）

ポートスキャンインスペクタの侵入ルールのオプション

`port_scan` 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。