Nmap App

Nmapは、ネットワーク検出とセキュリティ監査のための強力なユーティリティです。ネットワークをスキャンし、パケットを送信し、応答を解析し、スクリプトを実行して、ネットワークセキュリティを評価し、脆弱性を診断することができます。Nmapテストは、単一ホストまたは大規模ネットワークに対して実行できます。 Nmapテストは、自動テストおよびディスカバリアプリケーションと組み合わせて実行することもできます。

Nmap各章の内容

この章ではNmapテストについて、テストの作成方法、テスト設定の詳細、Nmap Runnerを使ったテストの実行方法、Nmap出力の例を説明します。

Nmapの紹介

Nmapは生のIPパケットを使用して以下の判断をします:

- ネットワーク上で利用可能なホスト
- ホストが提供するサービス（アプリケーション名とバージョン）
- 稼働しているオペレーティングシステム（およびバージョン）
- 使用されているパケットフィルターやファイアウォールの種類。

Nmapアプリは、Nmap機能強化に役立つNmapスクリプトに対応しています。これらのスクリプトには以下のものが含まれます:

- 定義済みNmapスクリプト
- 作成したユーザースクリプト
- ディスカバリアプリで使用するカスタムディスカバリスクリプト

Nmapは以下の用途に使用できます:

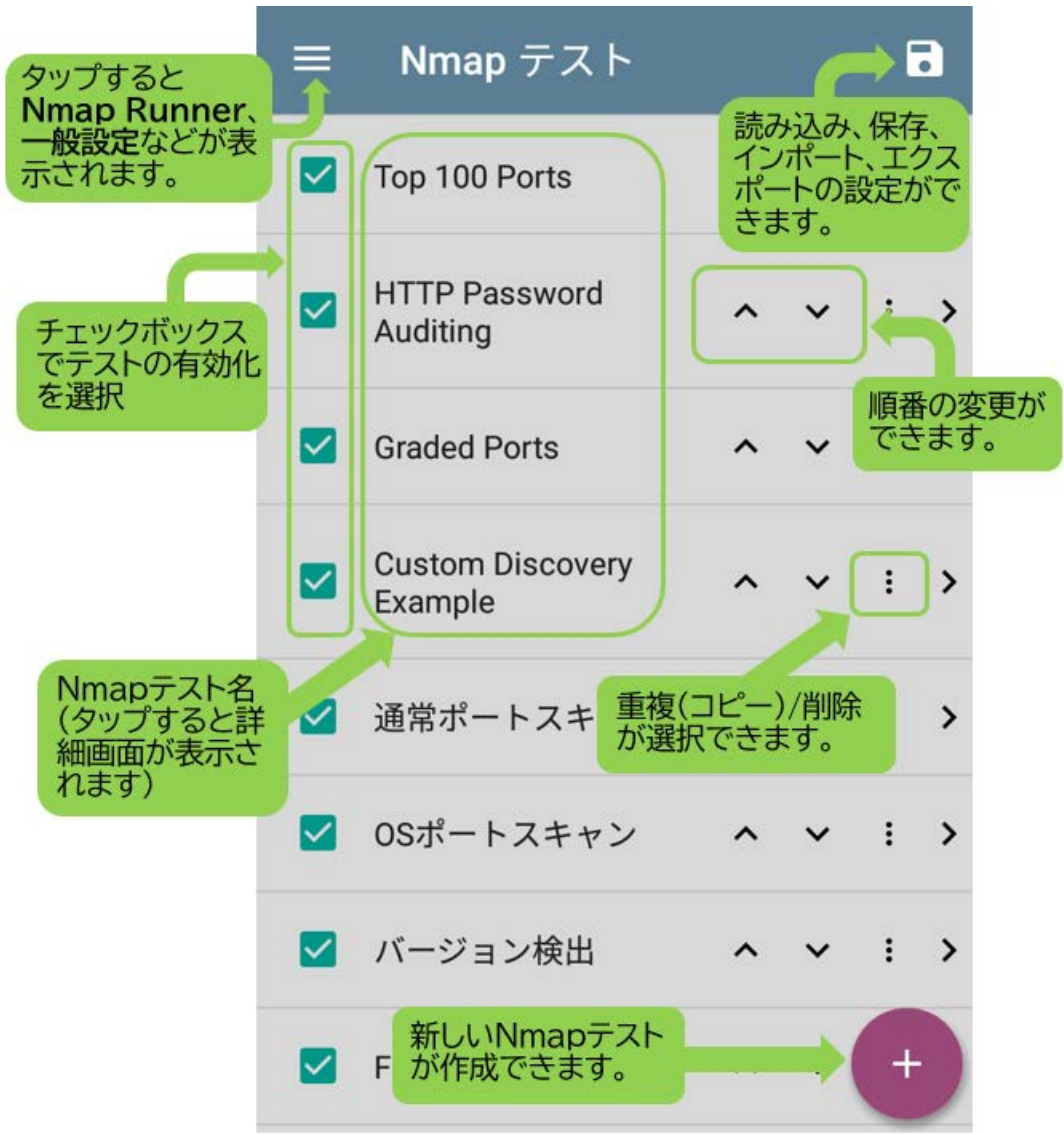
- どのようなネットワーク接続が可能かを調べることにより、デバイスやファイアウォールのセキュリティを監査します。
- ホスト上で開いているポートを特定します。

- ネットワークインベントリ、ネットワークマッピング、メンテナンスおよび資産管理
- ネットワーク上の新しいサーバを識別することによるセキュリティ監査
- ネットワークトラフィックをネットワークホストに送信し、応答と応答時間を解析します。
- ネットワークの脆弱性の発見
- DNSクエリの送信とサブドメインの検索
- サービスのアップグレードスケジュールの管理
- ホストまたはサービスのアップタイムの監視

Nmapに関するより詳細な情報は、Nmap.org.を参照してください。

Nmap テスト

Nmapテストのメイン画面には、NetAllyが提供する定義済みのデモテストと、作成またはインポートしたカスタムテストを含む Nmapテストの一覧が表示されます。



定義済みテスト

NetAllyでは、以下のような定義済みのNmap テストを提供しており、そのまま実行することも、コピーして独自の目的に合わせて変更することもできます。これらのテストは、テストユニットにおけるNmapの機能と能力の例を提供します。

Top 100 Ports：指定したターゲットで使用されている最も一般的な100ポートの情報をスキャンし、一覧表示します。

HTTP Password Auditing：Nmap テストにおけるスクリプトの使用例として、`http-brutescript` を使用してWebサーバ上のポート 80の認証をチェックし、必要に応じてブルートフォースパスワードテストを実行する例を示します。

Graded Ports：正規表現(regex)を使用して、値の範囲を含む必要があり、別の値のセットを含んではならない結果の等級付けやマークアップを行うことにより、正規表現の使用を示します。

Custom Discovery Example：ディスカバリアプリの一部として実行されるテストのデモです。テストを実行するための追加情報や引数を提供する場合があります。このサンプルテストは、`custom-discovery-example.nse` スクリプトのラッパーです。

サンプルスクリプトは、ディスカバリとスクリプト間のAPIを文書化したものです。この場合、ディスカバリはスクリプトの引数を提供します。ディスカバリテストは、ターゲットネットワーク上で検出することができるすべてのアドレスに対して実行することができ、ネットワーク管理者にとって強力な助けとなります。

その他のリスト操作

- チェックボックス  を選択すると、Nmap Runnerでテストの実行を**有効**/**無効**、リスト内でテストの移動操作を**有効**/**無効**にできます。また自動テストアプリとディスカバリアプでテストを利用できるようになります。
- 上下の矢印アイコン  をタップすることで、リスト内のテストを上下に移動できます。
- テストのアクションオーバーフローアイコンをタップ  すると、**重複**(コピー)/**削除**メニューが開きます:
    - 選択したテストをコピーするには、**重複**をタップします。Nmap Test画面が開き、テストのパラメータを変更および編集できます。コピーされたテストはテストリストに追加されます。

- 選択したテストを削除するには、**削除**をタップします。

新規テストの作成

新しいNmapテストを作成するには:

1. Nmapテストのメイン画面で、フローティング・アクション・アイコン をタップします。新しい空白のテストが作成され、Nmapテストのパラメータ画面が開きます。
2. テストのパラメータを編集するには、Nmapテストパラメータ画面を使用します。
3. システムの[**戻る**]アイコン をタップするか、ナビゲーション・メニュー・アイコン をタップして[**Nmap テスト**]を選択し、メインのテストリストに戻ると新しいテストがリストに含まれるようになります。
4. Nmap テストの実行を参照し、新しいテストを実行します。

アプリ設定の読み込み、保存、インポート、エクスポート

Nmapアプリのメイン画面の右上にある保存ボタン を押すと、以下の選択メニューが開きます:

- **読み込み**：以前に保存したNmap設定を開きます。
- **名前を付けて保存**：は、現在の設定を既存の名前または新しいカスタム名で保存します。
- インポートします： 前にエクスポートした設定ファイルをインポートします。
- **エクスポート**：現在の設定のエクスポートファイルを作成し、内部または接続された外部ストレージに保存します。
- **Link-Live へエクスポート**： 現在の設定をLink-Liveに直接エクスポートします。

Nmapテスト パラメータの編集

テストの基本パラメータを編集するには、Nmapテストメイン画面のリストでテストをタップするとNmapテスト画面が表示されます。

名前：テストの名前です。必要に応じて名前を編集します。

オプション：テストのNmapオプションです。(例えば、デフォルトのTop 100 Portsテストでは、**-sT --top-ports 100**がリストされています。) 必要に応じてオプションを編集します。

スクリプト：このフィールドをタップすると、スクリプト画面が表示されます。Nmapスクリプトの詳細については、https://nmap.org/nsedoc/scripts/を参照してください。

NOTE: お好みの環境で独自のNmapスクリプトを作成し、Link-Liveにアップロードして、Link-LiveのNmap機能を使用して、組織のCyberScopeユニットにスクリプトをプッシュできます。

- **スクリプトを使う**：タップし、スクリプトオプションを**有効**または**無効**にします。
- **名前**：フィールドをタップして、スクリプト名を入力します：
  1. テキストエディタを使用して、スクリプト名の頭文字を入力します。入力する、Nmapアプリが一致するスクリプトを表示します。
  2. 選択が完了したらOKをタップします。
- **引数(Arguments)**：タップしてスクリプトの引数を入力します。

タイムアウト：タップして無効にするか、プリセット値を選択します。カスタム値を入力することもできます。

結果に必須で含む：結果に含まなければならない値を指定します。グレーディング出力に使用します。フィールドをタップすると、文字列または正規表現値を入力するためのテキストエディタが開きます。例えば、Graded Portsのサンプルテストではこの値が使用されます：

```
regex:\n25/tcp +filtered +SMTP
```

結果に含まない：結果に含まれてはならない値を指定します。グレーディング出力に使用します。フィールドをタップしてテキストエディタを開き、文字列または正規表現値を入力します。

例えば、Graded Portsのサンプルテストではこの値が使用されます：

```
regex:\d+tcp +open
```

結果の評価：「**結果に必須で含む**」または「**結果に含まない**」パラメータの結果を指定するには、タップして**警告**または**エラー**のいずれかを選択します。例えば、サンプルテストの**HTTP Password Auditing**の出力結果は、オープンポートを**黄色**に着色して警告状態を示しています。

Advanced：フィールドをタップして、詳細オプション画面を開きます。

- **出力制限**：タップして出力制限または制限なしを選択します。
  NOTE: Nmapテストの中には、かなりの出力を生成するものがあるので、妥当な出力制限を設定することは、テスト結果を明確にするのに役立ちます。
- **認識されないFingerprintsを含む**：タップして、出力結果に認識されないオペレーティングシステムのfingerprintsを含めるかどうかを有効または無効にします。

テストタイプの変更

テストのタイプを標準Nmapテストとカスタムディスカバリテストの間で変更する必要がある場合は、

アクションオーバーフローメニューアイコン  をタップして、テストタイプオプションを開き、**テストタイプ**をタップします。ダイアログからテストの種類を選択します。

カスタムディスカバリテストについて：CyberScopeは、カスタムスクリプトを追加することで、検出されたデバイスを強化するためにこれらのテストを可能にします。典型的なアプリケーションは、企業のITシステムへの統合です。

API(GET)経由で追加情報を取得し、他のデバイスの詳細と一緒に結果を表示することで、CyberScope上で結果を装飾することができます。また、カスタムスクリプトを使用して、情報をAPI(PUT)にプッシュして、既存のITソフトウェアやアプリケーションを拡張することもできます。

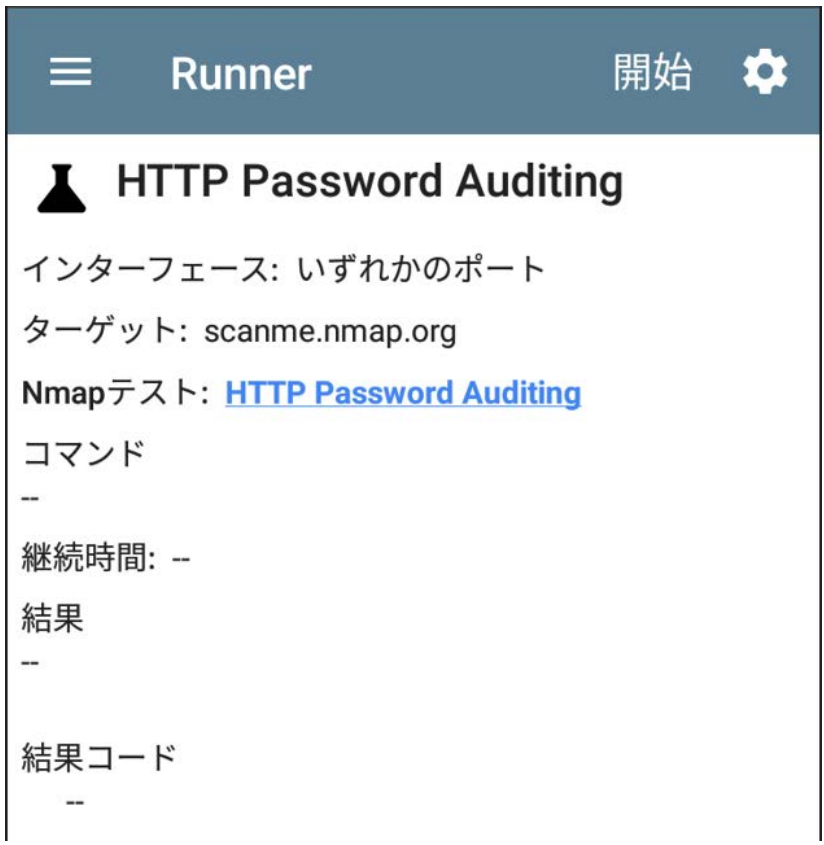
カスタム・ディスカバリ・スクリプトの開発は本ガイドの範囲外ですが、**Custom Discovery Example**では、CyberScopeでこのようなテストをどのように使用するかを理解するためのサンプルテストを提供しています。

正規表現のリソース

CyberScopeで使用される正規表現の形式については、正規表現構文チートシートを参照してください。

Nmapテストの実行

Nmap Runnerはテストの実行、実行設定を編集、結果をアップロードすることができます。



1. Nmapテストのメイン画面から、実行したいテストをタップします。Nmapテストパラメータ画面が開き、テストのパラメータを編集できます。
2. Nmapテスト画面を使ってテストのパラメータを編集します。

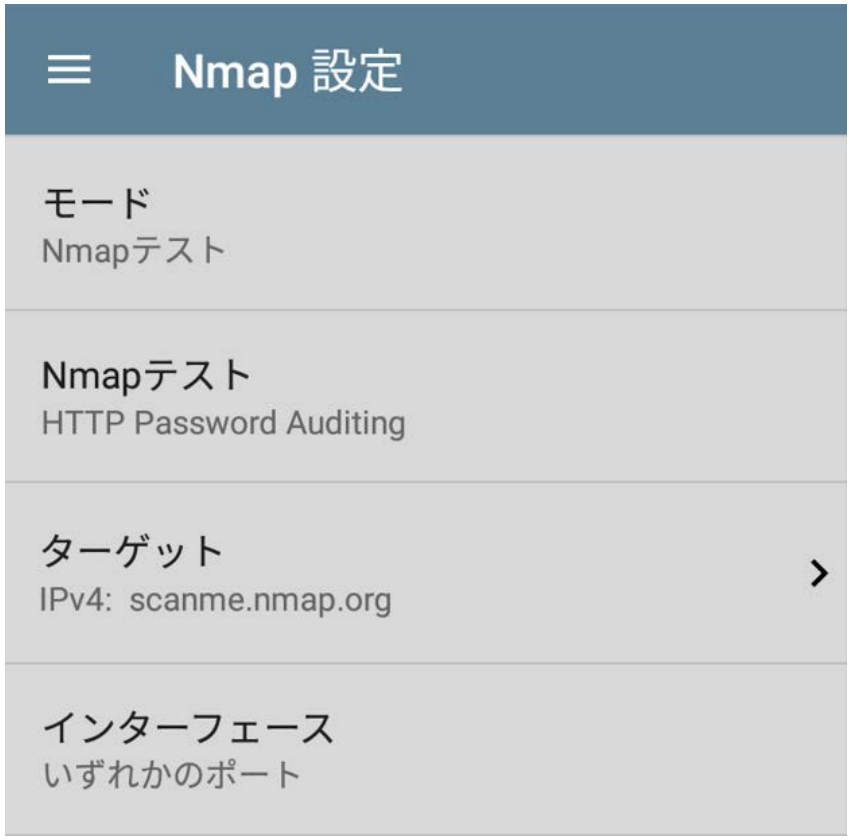
3. 必要なパラメータを変更したら、TESTをタップします。その後Runner画面が開きます。
4. アプリの設定アイコン  をタップしてNmap設定画面を開き、特定のテストの実行設定を編集します。(これには、テストにターゲットが必要な場合のターゲット指定も含まれます)。
NOTE: テスト名のリンクをタップしてNmapテスト画面に戻り、パラメータを編集できます。
5. システムの[**戻る**]アイコン  をタップして、Runner画面に戻ります。
6. **開始**をタップします。選択したパラメータと設定でテストが実行されます。
7. (オプション)アクション・オーバーフロー・アイコン  をタップし、**Link-Liveへアップロード**を選択して、テスト結果をLink-Liveクラウド・サービスにアップロードします。
    a. **コメント**フィールドにテストに関する任意のコメントを入力します。

b. **Job**コメントフィールドにテストや結果に関する任意の情報を入力します。

c. **Link-Live**に**保存**をタップします。

Nmap Runnerの設定

これらの Nmap Runner設定は、テストのランタイム設定を指定します。テストとともに保存される安定したテストパラメータとは対照的に、これらの設定はテストの実行ごとに変更される可能性があります。



モード

テストの実行方法を選択します。

Nmapテスト – Nmapテストで指定されたパラメータを使用してNmapコマンドを構築します。

コマンドライン - デフォルトのNmapコマンドから開始し、編集可能なコマンドラインでテストを実行します。このモードは、コマンドラインオプションに加えたい特定の変更がわかっている場合に便利です。

Nmapテスト

(**Nmapテストモードのみ**)

- 現在のテスト名を表示します。
- 新しいテストを選択します:
    1. テキストエディタを使用して、現在のテスト名を削除すると利用可能なテストのリストが表示されます。
    2. リストから新しいテストを選択し、**OK**をタップします。

ターゲット

(**Nmapテストモードのみ**) このフィールドをタップすると、**ターゲット**画面が表示されます。

NOTE: 全てのNmapテストがターゲットを必要とするわけではありません。

- **ターゲットを含む** - タップしてターゲットオプションを有効または無効にします。
- **ターゲット** - タップしてテキストフィールドを開き、ターゲット名を入力します。
  - 下矢印をタップして、**名前**（URLなど）または**IPアドレス**のいずれかを選択します。
  - フィールドに**名前**または**IPアドレス**を入力し、**OK**をタップします。
- **IP プロトコル Version** – **IPv4**または**IPv6**のいずれかをタップして選択します。

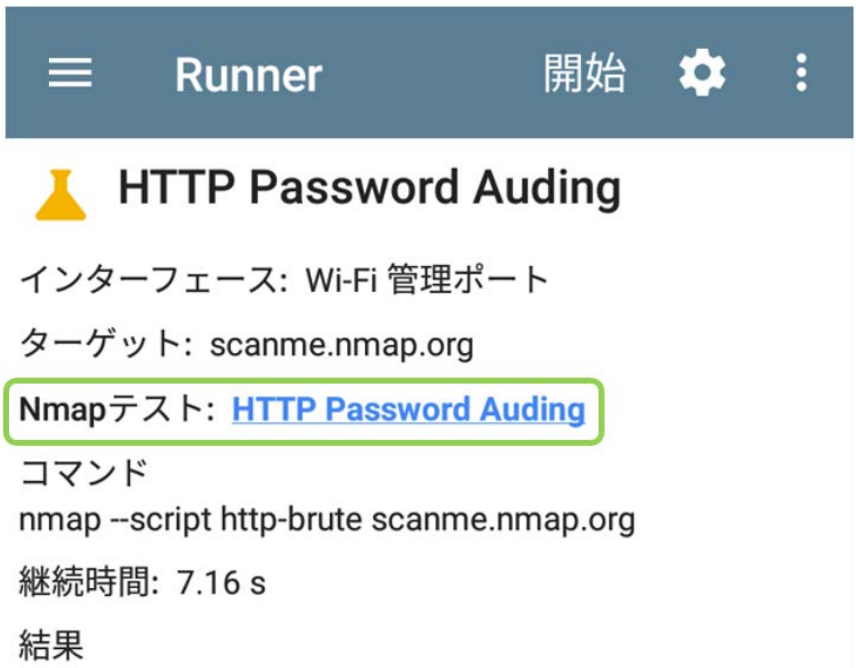
インターフェース

このフィールドをタップして、テストを実行するポート（**いずれか**、**有線**、**Wi-Fi**、**管理**など）を選択します。

Nmap 出力

このセクションでは、Nmap出力の詳細と、NetAlly Nmapパラメータを使用して出力の外観を向上させる方法の2つの例を示します。また、Nmap.orgに文書化されているように、Nmapユーティリティには多くの出力オプションがあります。

- 出力されたテスト名のリンクをタップすると、Nmapテストパラメータ画面が開き、新しいテスト実行のさまざまなオプションを編集できます。

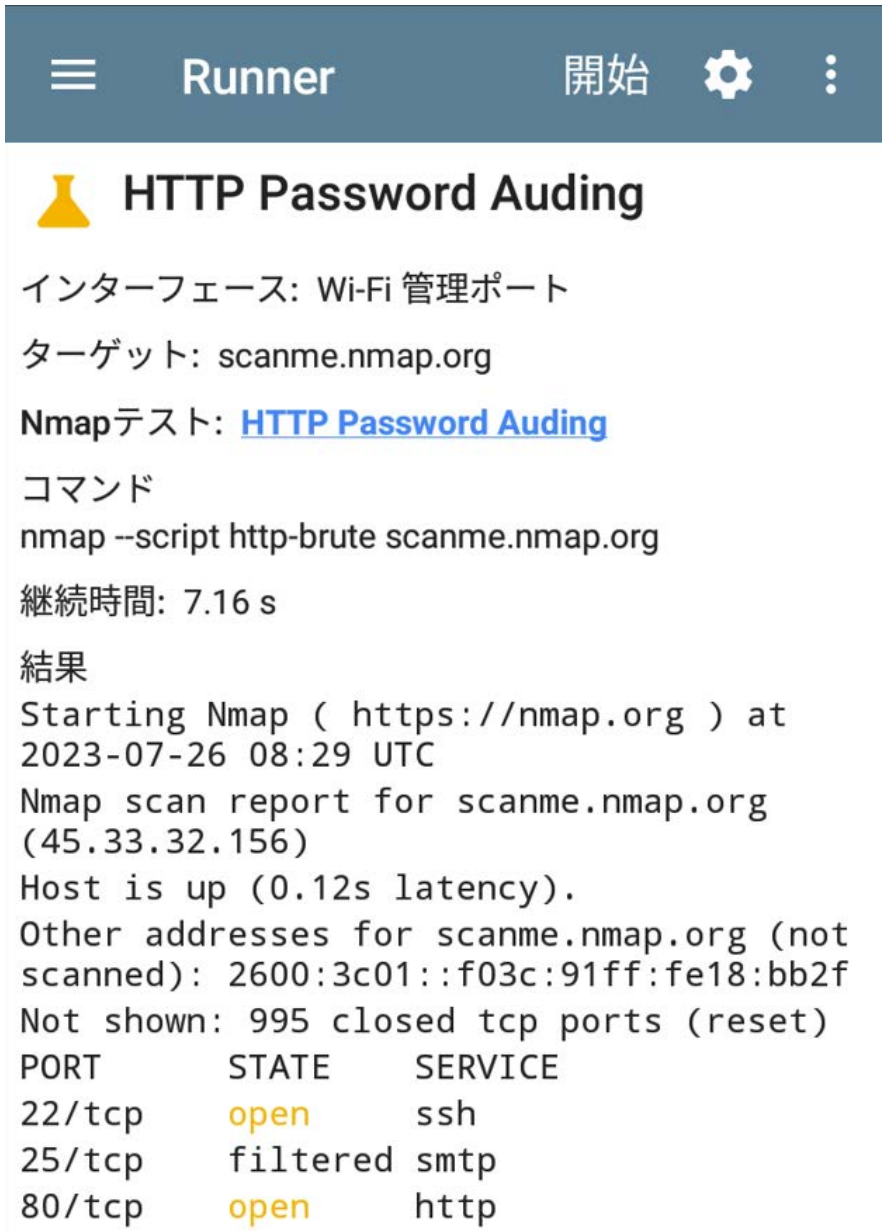


- 詳細オプションの**出力制限**パラメーターは出力サイズのコントロールができます。

- テスト結果をLink-Liveにアップロードするには、出力画面の上部にあるアクションオーバーフローアイコン  をタップし、「**Link-Liveへアップロード**」をタップします。 アップロード画面で必要なコメントやジョブコメントを入力し、「**LINK-LIVEに保存**」をタップします。

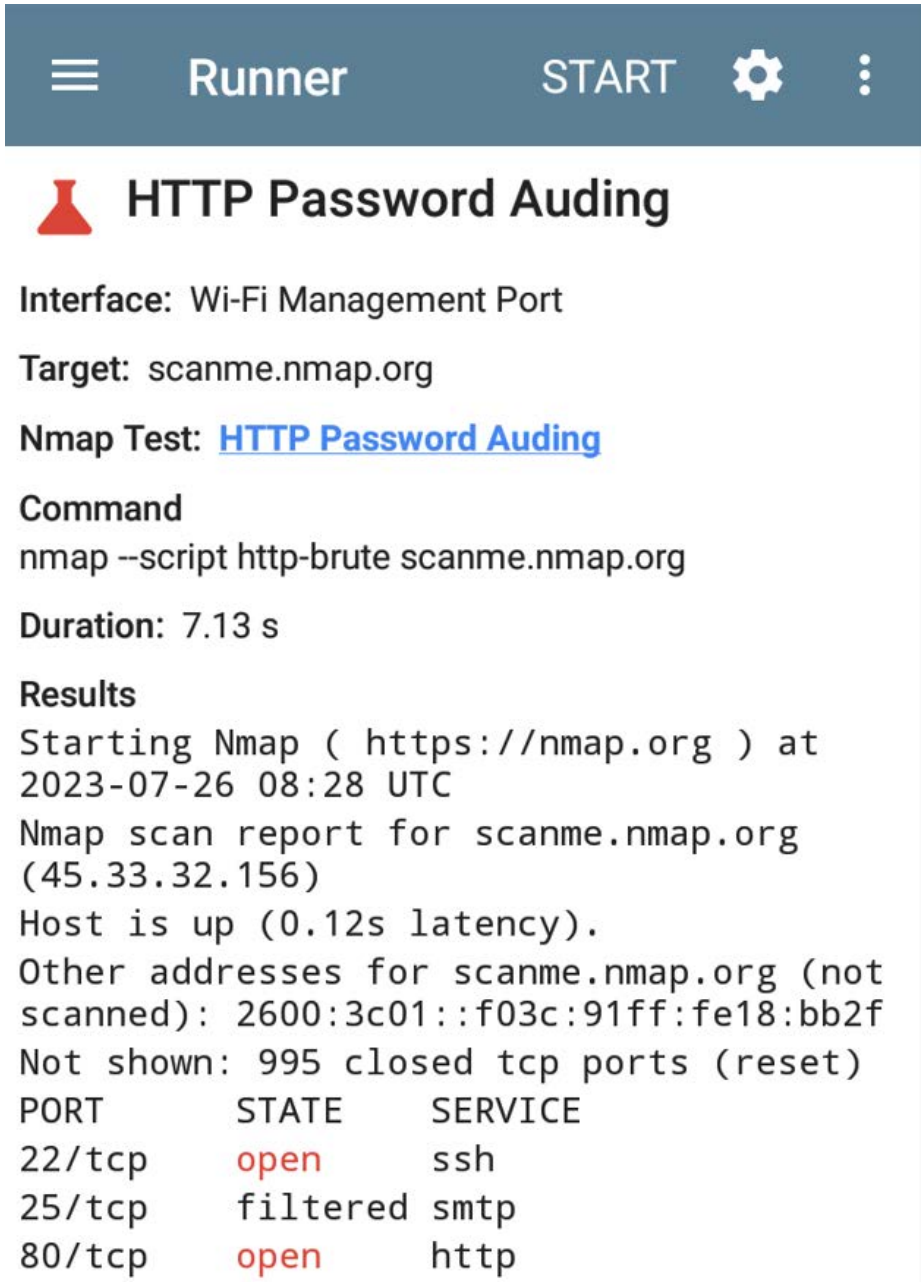
以下は、NetAlly Nmapのパラメータを使用して、出力の外観を評価および整理する方法の例です。

- **Password Audit with Result Grade Warning**：最初の例は、nmap.orgに対して実行されたサンプルHTTP Password Auditingテストの結果画面の一部を表示しています。「**結果に含まない**」パラメータにテキスト「**open**」が設定され、「**結果の評価**」パラメータに「**警告**」が設定されています。ポートの結果に"**open**"という文字が表示されると、出力結果の文字列と同様に、出力ヘッダーのアイコンが警告を示す**黄色**で表示されます。



- **Password Audit with Result Grade Error :** 2番目の例は、nmap.orgに対して実行されたサンプルHTTP Password Auditingテストの結果画面の一部を表示しています。

「**結果に含まない**」パラメータにもテキスト「**open**」が設定され、「**結果の評価**」パラメータには「**エラー**」が設定されています。ポート結果に"**open**"というテキストが表示されると、出力結果の文字列と同様に、出力ヘッダーのアイコンがエラーを示す**赤色**になります。



- **Password Audit with Regex Expression and Result Grade Error** : 最後の例では、HTTP Password Auditingテストで正規表現を使用し、出力を整理して評価する方法を示します。

「**結果に必須で含む**」パラメータを″`regex:PORT +STATE +SERVICE|[0-9]+ filtered|\d+ closed`″に設定し、出力結果の間隔を制御します。「**結果に含まない**」パラメータは″`regex:open +ssh`″に設定されていて、「**結果の評価**」パラメータが「**エラー**」に設定されています。以下の部分的な結果画面は、正規表現基準を満たしたために**緑色**に着色されたclosed portのデータを示しています。sshポートが開いていると、エラーが発生し、画面上部のNmapアイコンが**赤く**表示されます。

Top 100 Ports (test)

インターフェース: Wi-Fi 管理ポート

ターゲット: scanme.nmap.org

Nmapテスト: Top 100 Ports (test)

コマンド

```
nmap -sT --top-ports 100 scanme.nmap.org
```

継続時間: 2.06 s

結果

```
Starting Nmap ( https://nmap.org ) at
2023-07-27 01:56 UTC
Nmap scan report for scanme.nmap.org
(45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not
scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 97 closed tcp ports
(conn-refused)
PORT   STATE    SERVICE
22/tcp open     ssh
25/tcp filtered smtp
80/tcp open     http
```