03: ラボ03 - サポートラボ - オープンサービスポートの検索

Security+ (Exam SY0-701) JPN

Congratulations, you passed!

Duration: 34 minutes, 28 seconds

☑ このターゲットで開いているポートは何ですか？ *Score: 1*

- ☐ 21
- ☐ 22
- ☑ 25
- ☐ 53
- ☐ 80
- ☐ 443
- ☐ 3389

おめでとうございます！正解です。

☑ ターゲット上で検出されたOSは何ですか？ *Score: 1*

- ○ Linux
- ○ Windows
- ○ Unix
- ○ MacOS
- ◉ FreeBSD

おめでとうございます！正解です。

☑ **confirm Kali IP guest network address** *Score: 1*

このタスクを確認するには**Score（得点）**ボタンを選択します。
Kaliがゲストネットワークに接続されています。

☑ **confirm OPNsense service name** *Score: 1*

このタスクを確認するには**Score（得点）**ボタンを選択します。
サービス名が正しい。

☑ ターゲット上で発見されたOSは何ですか？ *Score: 1*

- ○ Linux

- ○ Windows
- ◉ FreeBSD
- ○ MacOS
- ○ Unix

おめでとうございます！正解です。

☑ **confirm Kali IP client network address** *Score: 1*

このタスクを確認するには**Score（得点）**ボタンを選択します。
Kali がクライアントネットワークに接続されています。

☑ このターゲット上でオープンポートからアクセス可能なサービスは何ですか？ *Score: 1*

- ☐ FTP
- ☑ SMTP
- ☑ HTTP
- ☑ msrpc
- ☐ NTP
- ☑ IMAP
- ☑ Microsoft-DS
- ☑ Mountd (つまり、NFS)
- ☑ MySQL
- ☐ RDP

おめでとうございます！正解です。

☑ 脅威ベクトルとは何ですか？ *Score: 1*

- ◉ 侵入を試みる可能性のある経路
- ○ エクスプロイト開発の進歩の矢印
- ○ 攻撃が発生する可能性のある年間回数
- ○ 違反による損害の重大性の評価

おめでとうございます！正解です。

☑ 攻撃対象領域とは何ですか？ *Score: 1*

- ◉ 暴露された脆弱性のコレクション
- ○ システム上のポートのリスト
- ○ サーバーのバックグラウンドで実行されているサービス
- ○ サーバーのシェル

おめでとうございます！正解です。

☑ サービス識別を表示するスキャンを実行するnmapパラメータオプションは？ *Score: 1*

- -oS
- -sS
- --banner
- -sV

おめでとうございます！正解です。

☑ 脅威はどこから発生するのでしょうか？ *Score: 1*

- 外部
- 内部
- サードパーティソフトウェア
- 上記のすべて

おめでとうございます！正解です。

☑ 安全でないサービスをホストしているオープンポートを発見した場合の主な2つの対応オプションは何ですか？ *Score: 1*

- [x] 公開したポートを閉じる
- [x] 暗号化の構成
- [ ] より複雑なパスワードを要求
- [ ] nmapを使用して脆弱性スキャンを実行する
- [ ] OSにアップデートを適用

おめでとうございます！正解です。